FORTRA

Active View Vulnerability Details Report

Report Data Source: Active View
Date Sourced:

Prepared for: Demo Account
Businessgroup: Enterprise Admins
Date Generated:
Data Options: Default | Include Acceptable Risk | 730 day window | Rating Method: DDI

Table of Contents

1 Identification and Purpose

Frontline provides an Active View of all assets that have been assessed. This document presents the most current findings across all of the assets that have been included in the scope of this report. The results in the sections below include high-level remarks about the security issues that were identified and general recommendations for improving the security posture of Demo Account.

This report on the current Active View was generated to highlight deficiencies in the patch level and security configuration of assets and to aid Demo Account in managing risk.

The following sections provide a summary of findings that includes the Security GPA for the assets that are within the scope of this report, and an overview of vulnerabilities at a high level. The next section contains a detailed report on the assets that were within the scope of the assessment. The last section contains high-impact recommendations for improving general security posture. An explanation of the ratings that are used throughout the report are provided in the appendix section.

2 Overview

This report provides a summary for Demo Account and covers 251 assets. The assets have 79 occurrences of 11 critical-severity vulnerabilities, 547 occurrences of 329 high-severity vulnerabilities, 588 occurrences of 323 medium-severity vulnerabilities, 406 occurrences of 59 low-severity vulnerabilities, and 3169 occurrences of 637 trivial-severity vulnerabilities.

Overall security posture: **C-**

Based on existing vulnerabilities, associated asset ratings, and assigned business risk of individual assets, the overall Security GPA for Demo Account is **1.35 (C-)**.

Data for this report is sourced from Active View as of . Details concerning the rating system are provided in the Appendix.

3 Asset Vulnerability Information

The severity attributed to each asset contributes to the overall security posture. The figures provided are intended to aid in performing a qualitative analysis of Demo Account security posture.

3.1 Comprehensive Asset Rating Overview

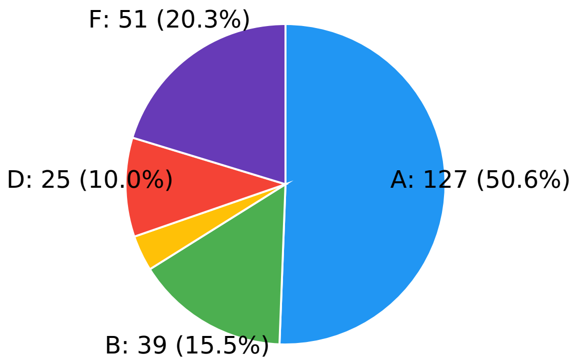

Figure 3.1: Number and percentage of assets covered by this report that have a given asset rating.

3.2 Vulnerability Counts by Severity

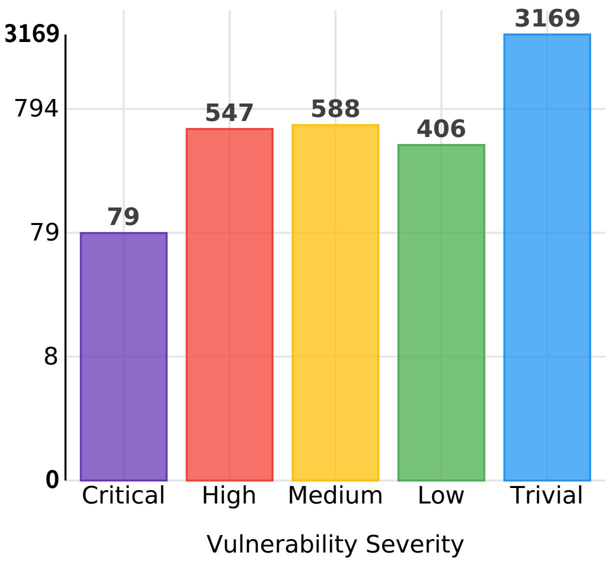

Figure 3.2: Number of vulnerabilities per Severity Rating that exist in the assets covered by this report.

3.3 Top 5 At Risk Assets

It is important to understand which of Demo Account's assets are most at risk. Table 3.3 shows the 5 assets which have the highest risk rating.

#	Rating	Hostname	Operating System	Vulns
1	F	BUFF-HEARTBLEED 192.168.69.106	Ubuntu Linux server	170
2	F	BUFF-HEARTBLEED 192.168.68.101	Ubuntu Linux server	165
3	F	BUFF-HEARTBLEED 192.168.67.55	Ubuntu Linux server	153
4	F	WINXP-ORACLE 192.168.67.62	Windows XP client	57
5	F	ATS-WIN7-ENT64 192.168.69.245	Windows 7 Enterprise client	43

Table 3.3 The 5 assets with the most severe rating are listed in this table.

4 Trending Information

Trending provides a quick and easy way to see how well you are doing over time.

4.1 Security GPA Trends

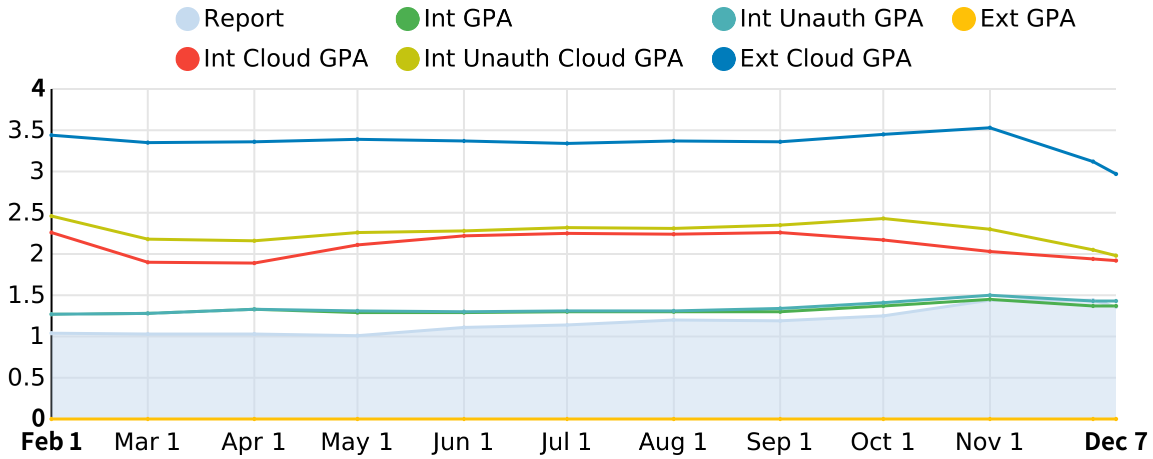

Figure 4.1: Security GPA trending graphs shows trends over the past year for all assets in this report.

4.2 Vulnerability Severity Trends

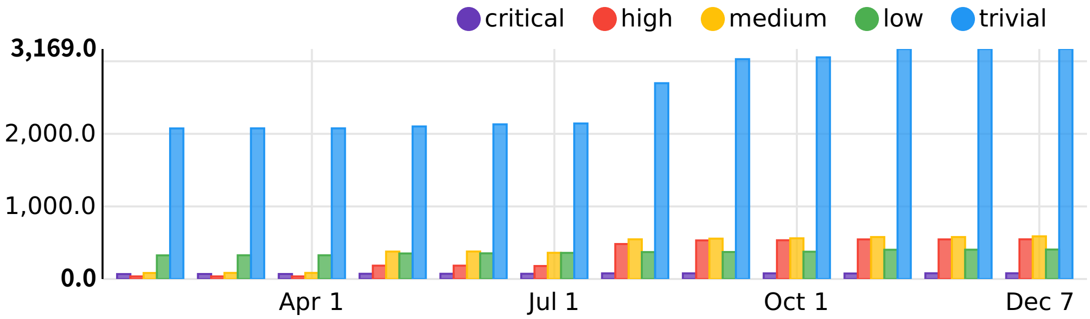

Figure 4.2: Vulnerability severity trending shows trends over the past year for all vulnerabilities in this report.

4.3 Vulnerability Status Trends

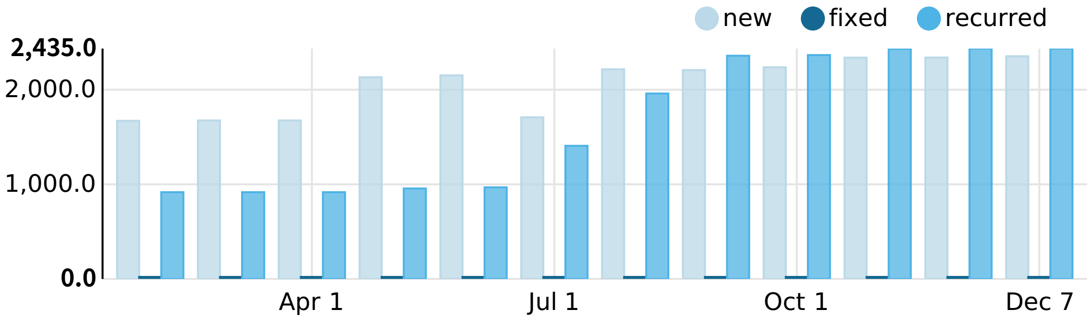

Figure 4.3: Vulnerability status trending shows trends over the past year for all vulnerabilities in this report.

5 Vulnerability Summary

This section covers 1359 unique vulnerabilities. A summary of the unique vulnerability counts and their associated instance counts are located below followed by a list of each unique vulnerability within the scope of this report.

Severity Counts Breakdown					
Severity	Critical	High	Medium	Low	Trivial
Unique:	11	329	323	59	637
Instances:	79	547	588	406	3169

Vulnerability Title	Count	Severity
Easily Guessable SSH Credentials (104120)	27	Critical
SSL Connection: Server Vulnerable to Heartbleed Attack (113790)	15	Critical
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051)	14	Critical
MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831)	6	Critical
Emerson Avocent Default SSH Credentials (118921)	3	Critical
MS08-067 Microsoft Windows Server Service Stack Overflow (Network Check) (103802)	3	Critical
MS09-050 Microsoft Windows SMB2 Command Execution Vulnerabilities (Network Check) (104045)	3	Critical
Unix Server Common Password (100151)	3	Critical
Samba IsKnownPipename Remote Code Execution (122062)	2	Critical
Threat Detected: Trojan Variant (126460)	2	Critical
HTTP Easily Guessable Credentials (104433)	1	Critical
Microsoft Windows 7 End of Life (131864)	8	High

MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735)	7	High
OpenSSH 'ssh-agent' Double Free Vulnerability (144213)	7	High
MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) (117590)	6	High
MS22-JUL: Microsoft Windows Security Update (149222)	5	High
Apache HTTP Server 'mod_proxy_ftp' Uninitialized Memory Usage Vulnerability (133605)	4	High
Apache HTTP Server Security Update 2.4.48 (145498)	4	High
MS21-DEC: Microsoft Windows Security Update (147272)	4	High
MS22-APR: Microsoft Windows Security Update (148319)	4	High
MS22-FEB: Microsoft Windows Security Update (147753)	4	High
MS22-JAN: Microsoft Windows Security Update (147420)	4	High
MS22-JUN: Microsoft Windows Security Update (148994)	4	High
MS22-MAR: Microsoft Windows Security Update (148037)	4	High
MS22-MAY: Microsoft Windows Security Update (148572)	4	High
Apache HTTP Server 2.4.53 Security Release (148390)	3	High
Apache HTTP Server Security Update 2.4.51 (147293)	3	High
Microsoft Windows Server 2008 End of Life (131869)	3	High
Microsoft Windows XP End of Life (113789)	3	High
MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Registry Entry Not Set (149637)	3	High
Apache httpd '2.2.32 2.4.24' Remote Segmentation Fault Vulnerability (290291)	2	High
Apache httpd '2.2.x before 2.2.33 and 2.4.x before 2.4.26' 'mod_mime' subcomponent Remote Read Vulnerability (290301)	2	High

Apache httpd '2.2.x before 2.2.33' and '2.4.x before 2.4.26' 'mod_ssl' subcomponent NULL pointer Vulnerability (290295)	2	High
Apache HTTP Server 'ap_get_basic_auth_pw' Authentication Bypass (290284)	2	High
Apache HTTP Server Internal Data Buffering Denial of Service Vulnerability (129589)	2	High
Apache HTTP Server 'Module Scripts' Privilege Escalation Vulnerability (128443)	2	High
MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (116972)	2	High
MS15-009: Security Update for Internet Explorer (117381)	2	High
MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (117380)	2	High
MS15-018: Cumulative Security Update for Internet Explorer (117479)	2	High
MS15-021: Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (117476)	2	High
MS15-032: Cumulative Security Update for Internet Explorer (117588)	2	High
MS15-043: Cumulative Security Update for Internet Explorer (117738)	2	High
MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (117737)	2	High
MS15-056: Cumulative Security Update for Internet Explorer (117878)	2	High
MS15-065: Security Update for Internet Explorer (118050)	2	High
MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (118096)	2	High
MS15-079: Cumulative Security Update for Internet Explorer (118134)	2	High
MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (118133)	2	High
MS15-093: Security Update for Internet Explorer (118245)	2	High
MS15-106: Cumulative Security Update for Internet Explorer (118394)	2	High

MS15-124: Cumulative Security Update for Internet Explorer (118670)	2	High
MS16-001: Cumulative Security Update for Internet Explorer (118689)	2	High
MS16-009: Cumulative Security Update for Internet Explorer (118985)	2	High
MS16-012: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (118984)	2	High
MS16-023: Cumulative Security Update for Internet Explorer (119094)	2	High
MS16-028: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (119089)	2	High
MS16-037: Cumulative Security Update for Internet Explorer (119278)	2	High
MS16-039: Security Update for Microsoft Graphics Component (119276)	2	High
MS16-040: Security Update for Microsoft XML Core Services (119275)	2	High
MS16-063: Cumulative Security Update for Internet Explorer (119505)	2	High
MS16-087: Security Update for Windows Print Spooler Components (119630)	2	High
MS16-095: Cumulative Security Update for Internet Explorer (119722)	2	High
MS16-104: Cumulative Security Update for Internet Explorer (120918)	2	High
MS16-116: Security Update in OLE Automation for VBScript Scripting Engine (120906)	2	High
MS16-118: Cumulative Security Update for Internet Explorer (121027)	2	High
MS16-130: Security Update for Microsoft Windows (121132)	2	High
MS16-132: Security Update for Microsoft Graphics Component (121130)	2	High
MS16-144: Cumulative Security Update for Internet Explorer (121327)	2	High
MS16-146: Security Update for Microsoft Graphics Component (121325)	2	High
MS16-147: Security Update for Microsoft Uniscribe (121324)	2	High

MS17-006: Cumulative Security Update for Internet Explorer (121910)	2	High
MS17-010: Security Update for Microsoft Windows SMB Server (121906)	2	High
MS17-013: Security Update for Microsoft Graphics Component (121903)	2	High
MS17-APR: Microsoft Internet Explorer Security Update (122044)	2	High
MS17-APR: Microsoft .NET Security Update (122049)	2	High
MS17-APR: Microsoft Windows Security Update (122045)	2	High
MS17-AUG: Microsoft Windows Security Update (122397)	2	High
MS17-DEC: Microsoft Internet Explorer Security Update (123543)	2	High
MS17-DEC: Microsoft Windows Security Update (123544)	2	High
MS17-JUL: Microsoft Internet Explorer Security Update (122295)	2	High
MS17-JUL: Microsoft Windows Security Update (122296)	2	High
MS17-JUN: Microsoft Windows Security Update (122281)	2	High
MS17-MAY: Microsoft Internet Explorer Security Update (122153)	2	High
MS17-MAY: Microsoft Windows Security Update (122154)	2	High
MS17-NOV: Microsoft Internet Explorer Security Update (122791)	2	High
MS17-OCT: Microsoft Internet Explorer Security Update (122637)	2	High
MS17-OCT: Microsoft Windows Security Update (122638)	2	High
MS17-SEP: Microsoft Internet Explorer Security Update (122554)	2	High
MS17-SEP: Microsoft Windows Security Update (122555)	2	High
MS18-APR: Microsoft Internet Explorer Security Update (123954)	2	High
MS18-APR: Microsoft Windows Security Update (123955)	2	High
MS18-AUG: Microsoft Internet Explorer Security Update (125931)	2	High

MS18-AUG: Microsoft Windows Security Update (125932)	2	High
MS18-DEC: Microsoft Internet Explorer Security Update (127240)	2	High
MS18-DEC: Microsoft Windows Security Update (127241)	2	High
MS18-FEB: Microsoft Internet Explorer Security Update (123787)	2	High
MS18-FEB: Microsoft Windows Security Update (123788)	2	High
MS18-JAN: Microsoft Internet Explorer Security Update (MELTDOWN) (123602)	2	High
MS18-JUL: Microsoft Internet Explorer Security Update (125653)	2	High
MS18-JUL: Microsoft Windows Security Update (125654)	2	High
MS18-JUN: Microsoft Internet Explorer Security Update (125543)	2	High
MS18-JUN: Microsoft Windows Security Update (125544)	2	High
MS18-MAR: Microsoft Internet Explorer Security Update (123855)	2	High
MS18-MAR: Microsoft Windows Security Update (123856)	2	High
MS18-MAY: Microsoft Internet Explorer Security Update (124365)	2	High
MS18-MAY: Microsoft Windows Security Update (124366)	2	High
MS18-NOV: Microsoft Windows Security Update (126949)	2	High
MS18-OCT: Microsoft Internet Explorer Security Update (126601)	2	High
MS18-OCT: Microsoft Windows Security Update (126602)	2	High
MS18-SEP: Microsoft Internet Explorer Security Update (126400)	2	High
MS18-SEP: Microsoft Windows Security Update (126401)	2	High
MS19-APR: Microsoft Internet Explorer Security Update (128575)	2	High
MS19-APR: Microsoft Windows Security Update (128576)	2	High
MS19-AUG: Microsoft Internet Explorer Security Update (129475)	2	High

MS19-AUG: Microsoft Windows Security Update (129476)	2	High
MS19-DEC: Microsoft Internet Explorer Security Update (131866)	2	High
MS19-DEC: Microsoft Windows Security Update (131867)	2	High
MS19-FEB: Microsoft Internet Explorer Security Update (128001)	2	High
MS19-FEB: Microsoft Windows Security Update (127998)	2	High
MS19-JAN: Microsoft Windows Security Update (127739)	2	High
MS19-JUL: Microsoft Internet Explorer Security Update (129102)	2	High
MS19-JUL: Microsoft Windows Security Update (129103)	2	High
MS19-JUN: Microsoft Internet Explorer Security Update (128961)	2	High
MS19-JUN: Microsoft Windows Security Update (128962)	2	High
MS19-MAR: Microsoft Internet Explorer Security Update (128289)	2	High
MS19-MAR: Microsoft Windows Security Update (128290)	2	High
MS19-MAY: Microsoft Internet Explorer Security Update (128794)	2	High
MS19-MAY: Microsoft Windows Security Update (ZombieLoad) (128795)	2	High
MS19-NOV: Microsoft Internet Explorer Security Update (131730)	2	High
MS19-NOV: Microsoft Windows Security Update (131731)	2	High
MS19-OCT: Microsoft Internet Explorer Security Update (129805)	2	High
MS19-OCT: Microsoft Windows Security Update (129806)	2	High
MS19-SEP: Microsoft Internet Explorer Out-of-Band Security Update (129724)	2	High
MS19-SEP: Microsoft Internet Explorer Security Update (129632)	2	High
MS19-SEP: Microsoft Windows Security Update (129633)	2	High

MS20-APR: Microsoft Internet Explorer Security Update (133730)	2	High
MS20-APR: Microsoft Windows Security Update (133731)	2	High
MS20-AUG: Microsoft Internet Explorer Security Update (138006)	2	High
MS20-AUG: Microsoft Windows Security Update (138007)	2	High
MS20-DEC: Microsoft Windows Security Update (143512)	2	High
MS20-FEB: Microsoft Internet Explorer Security Update (132515)	2	High
MS20-FEB: Microsoft Windows Security Update (132516)	2	High
MS20-JAN: Microsoft Internet Explorer Security Update (132229)	2	High
MS20-JAN: Microsoft Windows Security Update (132230)	2	High
MS20-JUL: Microsoft Internet Explorer Security Update (137511)	2	High
MS20-JUL: Microsoft Windows Security Update (137512)	2	High
MS20-JUN: Microsoft Internet Explorer Security Update (137199)	2	High
MS20-JUN: Microsoft Windows Security Update (137200)	2	High
MS20-MAR: Microsoft Internet Explorer Security Update (132714)	2	High
MS20-MAR: Microsoft Windows Security Update (132715)	2	High
MS20-MAY: Microsoft Internet Explorer Security Update (133999)	2	High
MS20-MAY: Microsoft Windows Security Update (134000)	2	High
MS20-NOV: Microsoft Internet Explorer Security Update (143188)	2	High
MS20-NOV: Microsoft Windows Security Update (143189)	2	High
MS20-OCT: Microsoft Windows Security Update (142682)	2	High
MS20-SEP: Microsoft Internet Explorer Security Update (138218)	2	High
MS20-SEP: Microsoft Windows Security Update (138219)	2	High

MS21-APR: Microsoft Windows Security Update (144750)	2	High
MS21-AUG: Microsoft Internet Explorer Security Update (146092)	2	High
MS21-AUG: Microsoft Windows Security Update (146090)	2	High
MS21-FEB: Microsoft Windows Security Update (144007)	2	High
MS21-JAN: Microsoft Windows Security Update (143778)	2	High
MS21-JUL: Microsoft Windows Out-of-Band Security Update (145515)	2	High
MS21-JUL: Microsoft Windows Security Update (145614)	2	High
MS21-JUN: Microsoft Windows Security Update (145281)	2	High
MS21-MAR: Microsoft Internet Explorer Security Update (144193)	2	High
MS21-MAR: Microsoft Windows Security Update (144194)	2	High
MS21-MAY: Microsoft Internet Explorer Security Update (144993)	2	High
MS21-MAY: Microsoft Windows Security Update (144994)	2	High
MS21-NOV: Microsoft Windows Security Update (146938)	2	High
MS21-OCT: Microsoft Internet Explorer Security Update (146692)	2	High
MS21-OCT: Microsoft Windows Security Update (146693)	2	High
MS21-SEP: Microsoft Internet Explorer Security Update (146369)	2	High
MS21-SEP: Microsoft Windows Security Update (146370)	2	High
MS22-JUN: Microsoft SQL Server Security Update (148996)	2	High
MS22-MAR: Microsoft Internet Explorer Security Update (148036)	2	High
OpenSSH Security Bypass Vulnerability (126647)	2	High
OpenSSH 'session.c' Local Security Bypass Vulnerability (126635)	2	High
OpenSSH 'ssh-agent.c' Untrusted Search Path Vulnerability (283439)	2	High

OpenSSH 'ssh/kex.c' Denial of Service Vulnerability (126638)	2	High
Windows 10 End of Life (125528)	2	High
Windows EFSRPC NTLM Relay Vulnerability (PetitPotam) (146093)	2	High
Apache Chunked Encoding Buffer Overflow (101470)	1	High
Apache Tomcat "Ghostcat" AJP Local File Inclusion and RCE (132639)	1	High
Apache Win32 Directory Traversal (101929)	1	High
Easily Guessable MySQL Credentials (104829)	1	High
Easily Guessable Telnet Credentials (111915)	1	High
Fileinfo 'file_check_mem' Arbitrary Code Execution (277148)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 100.0.1185.29 (148268)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 100.0.1185.36 (148266)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 100.0.1185.44 (148439)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 101.0.1210.32 (148544)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 101.0.1210.47 (148761)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 102.0.1245.30 (148969)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 102.0.1245.39 (148968)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 102.0.1245.41 (148970)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 103.0.1264.37 (149068)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 103.0.1264.44 (149202)	1	High

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 103.0.1264.49 (149201)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 92.0.902.78 (146249)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.38 (146375)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.44 (146376)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.47 (146377)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.52 (146565)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 94.0.992.31 (146566)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 94.0.992.38 (146671)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 94.0.992.47 (146670)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 95.0.1020.30 (146797)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 95.0.1020.40 (146924)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 96.0.1054.29 (147105)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 96.0.1054.57 (147257)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 97.0.1072.55 (147417)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 97.0.1072.69 (147752)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 98.0.1108.43 (147751)	1	High

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 98.0.1108.50 (148025)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 98.0.1108.55 (148026)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 99.0.1150.30 (148024)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 99.0.1150.46 (148265)	1	High
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 99.0.1150.55 (148267)	1	High
Microsoft Windows Server 2008 R2 End of Life (131870)	1	High
MS19-JUL: Microsoft SQL Server Security Update (129105)	1	High
MS20-FEB: Microsoft SQL Server Security Update (132519)	1	High
MS20-NOV: Microsoft Windows Security Update - Registry Entry Not Set (143527)	1	High
OpenSSH 'kbdint_next_device' Function Denial of Service (273895)	1	High
OpenSSH X11 Forwarding Access Bypass (276485)	1	High
PHP bcmath.c 'bcpowmod' Modified Data Structure Denial of Service (277158)	1	High
PHP bcmath.c 'bcpowmod' Negative Integer Denial of Service (277157)	1	High
PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 'get_icu_value_internal' Function Denial of Service (280827)	1	High
PHP before 5.5.36 and 5.6.x before 5.6.22 'file.c' Denial of Service (280830)	1	High
PHP before 5.5.36 and 5.6.x before 5.6.22 'php_escape_html_entities_ex' Function Denial of Service (280829)	1	High
PHP before 5.5.36 and 5.6.x before 5.6.22 'php_html_entities' Function Denial of Service (280828)	1	High
PHP CGI Component Command Execution Vulnerability (269957)	1	High

PHP 'curl_file.c' CURLFile Implementation Denial of Service (283441)	1	High
PHP 'dynamicGetbuf' Denial of Service Vulnerability (127020)	1	High
PHP 'enchant_broker_request_dict' Function Arbitrary Code Execution (271564)	1	High
PHP 'escapeshellarg' Function Remote Command Execution Vulnerability (278617)	1	High
PHP exif.c 'exif_process_IFD_in_JPEG' Denial of Service (277163)	1	High
PHP exif.c 'exif_process_IFD_TAG' Denial of Service (277162)	1	High
PHP exif.c 'exif_process_TIFF_in_JPEG' Denial of Service (277164)	1	High
PHP 'exif_process_IFD_in_MAKERNOTE' Denial of Service (277646)	1	High
PHP 'exif_process_IFD_in_TIFF' Uninitialized Read Vulnerability (128707)	1	High
PHP 'ext/phar/phar_object.c' Zero-length Uncompress Denial of Service (277155)	1	High
PHP 'ext/soap/soap.c' Type Confusion Vulnerability (272810)	1	High
PHP 'ext/spl/spl_array.c' Use-after-free Remote Code Execution (275416)	1	High
PHP ext/standard/http_fopen_wrapper.c 'php_stream_url_wrap_http_ex' Stack-based Buffer Under-read (901430)	1	High
PHP File Extension Restriction Bypass (272803)	1	High
PHP Fileinfo Component 'apprentice_load' Denial of Service Flaw (269855)	1	High
PHP Fileinfo Component Crafted ELF File Denial of Service (271569)	1	High
PHP 'ftp_genlist' Function Heap Buffer Overflow (272817)	1	High
PHP 'ftp_genlist' Function LIST Command Buffer Overflow (273431)	1	High
PHP gd.c 'imagegammacorrect' Input Validation Denial of Service Vulnerability (281188)	1	High

PHP gd.c 'imagetruecolortopalette' Input Validation Denial of Service Vulnerability (282235)	1	High
PHP 'gd_webp.c' Denial of Service Vulnerability (127034)	1	High
PHP grapheme.c 'grapheme_stripos' Denial of Service (277160)	1	High
PHP grapheme_string.c 'graphme_strpos' Denial of Service (277161)	1	High
PHP Heap-Based Buffer Over-Read Vulnerability (127909)	1	High
PHP IMAP PHP Extension 'phar_fix_filepath' Function Buffer Overflow Vulnerability (275412)	1	High
PHP 'incomplete_class.c' Type Confusion Denial of Service (273414)	1	High
PHP Invalid Memory Access Vulnerability (127908)	1	High
PHP 'locale_accept_from_http' Denial of Service (277459)	1	High
PHP 'locale_methods.c' Argument Overflow Denial of Service (283453)	1	High
PHP mbfilter.c 'mbfl_strcut' Integer Overflows Denial of Service (277154)	1	High
PHP mcrypt.c Multiple Integer Overflow Vulnerabilities (280834)	1	High
PHP Multiple Heap-Based Buffer Over-Read Vulnerabilities (127911)	1	High
PHP Multiple Type Confusion Denial of Service Vulnerabilities (273413)	1	High
PHP OPcache Extension '_zend_shared_memdup' Function Denial of Service Flaw (271046)	1	High
PHP Pathname Sanitization Remote Arbitrary File Access Vulnerability (273410)	1	High
PHP 'pcntl_exec' Implementation File Extension Restriction Bypass (272809)	1	High
PHP phar.c 'phar_parse_pharfile' Denial of Service (284034)	1	High
PHP Phar Extension 'phar_analyze_path' Arbitrary Code Execution (277153)	1	High

PHP phar_object.c 'phar_convert_to_other' Denial of Service (275411)	1	High
PHP 'phar_parse_metadata' Function Denial of Service (272818)	1	High
PHP "phar_rename_archive" Function Denial of Service Flaw (271566)	1	High
PHP 'phar_set_inode' Function Stack Buffer Overflow (272067)	1	High
PHP 'php_date.c' Multiple Use-After-Free Arbitrary Code Execution Flaws (271568)	1	High
PHP php_http.c 'make_http_soap_request' Remote Code Execution (276912)	1	High
PHP php_mbregex.c '_php_mb_regex_ereg_replace_exec' Double Free Vulnerability (280833)	1	High
PHP 'php_snmp_error' Function Format String Arbitrary Code Execution (277152)	1	High
PHP 'php_url_parse_ex' Denial of Service (277705)	1	High
PHP php_zip.c 'getFromIndex', 'getFromName' Heap Overflow (277149)	1	High
PHP php_zip.c Zip Extension Denial of Service (280836)	1	High
PHP 'process_nested_data' Function Use-After-Free Flaw (270531)	1	High
PHP 'process_nested_data' Function Use-After-Free Remote Code Execution Flaw (271575)	1	High
PHP sanitizing.c 'php_filter_encode' Integer Overflow Denial of Service (279636)	1	High
PHP 'sapi/fpm/fpm/fpm_unix.c' Privilege Escalation Vulnerability (126975)	1	High
PHP 'Serializable Interface, SplObjectStorage class, SplDoublyLinkedList class' Multiple Use-after-free Remote Code Execution (275414)	1	High
PHP 'session.c' Denial of Service (277689)	1	High
PHP Session Deserializer 'php_var_unserialize' Remote Code Execution (275415)	1	High

PHP 'simplestring_addn' Denial of Service Vulnerability (127019)	1	High
PHP 'snmp.c' Denial of Service (277774)	1	High
PHP SoapClient Multiple Type Confusion Denial of Service Vulnerabilities (273412)	1	High
PHP soap.c 'SoapClient__call' Arbitrary Code Execution (275418)	1	High
PHP 'soap.c' Type Confusion Denial of Service (273411)	1	High
PHP spl_array.c SplArray Unserialization Denial of Service (281201)	1	High
PHP spl_array.c 'SPL Extension' Denial of Service (280835)	1	High
PHP SPL 'ArrayObject, SplObjectStorage, SplDoublyLinkedList' Multiple Use-after-free Remote Code Execution (275413)	1	High
PHP SPL Component Type Confusion Vulnerability (265283)	1	High
PHP spl_directory.c 'SplFileObject::fread' Denial of Service (282146)	1	High
PHP spl_observer.c SplObjectStorage Unserialize Implementation Denial of Service (283532)	1	High
PHP 'spl_ptr_heap_insert' Function Arbitrary Code Execution Vulnerability (278838)	1	High
PHP string.c 'str_pad' Denial of Service (280596)	1	High
PHP 'tar.c' Stack Buffer Overflow (276915)	1	High
PHP 'uncompressed_filesize' Crafted PHAR Archive Denial of Service Vulnerability (281199)	1	High
PHP 'var_unserializer.c' Integer Overflow (268708)	1	High
PHP var_unserializer.c Invalid Object Denial of Service Vulnerability (281186)	1	High
PHP var_unserializer.re 'finish_nested_data' Buffer Overlow (292863)	1	High
PHP var_unserializer.re Object Deserialization Denial of Service (281197)	1	High
PHP 'var_unserializer.re' Use-after-free Vulnerability (269724)	1	High

PHP Wakeup Processing Denial of Service (283455)	1	High
PHP wddx.c 'php_wddx_process_data' Denial of Service Vulnerability (281190)	1	High
PHP wddx.c 'php_wddx_process_data' Double Free Vulnerability (280837)	1	High
PHP wddx.c 'wddx_stack_destroy' Denial of Service Vulnerability (281194)	1	High
PHP 'wddx.c' XML Document Denial of Service (283454)	1	High
PHP WDDX Extension Use-after-free Vulnerability (276916)	1	High
PHP xml.c 'xml_parse_into_struct' Denial of Service (277159)	1	High
PHP xml.c 'xml_utf8_encode' Integer Overflow Denial of Service (279482)	1	High
PHP Zend Engine 'zend_ts_hash_graceful_destroy' Function Denial of Service Flaw (269858)	1	High
PHP 'zend_exceptions.c' Type Confusion Remote Code Execution (273415)	1	High
PHP zend_string_extend in 'Zend/zend_string.h' Denial of Service (288890)	1	High
PHP ZIP Extension "_zip_cdir_new" Function Integer Overflow (271576)	1	High
Ruby 'Oniguruma-mod' and PHP fetch_token in 'mbstring' Denial of Service (289398)	1	High
Ruby 'Oniguruma-mod' and PHP 'mbstring' Denial of Service (289391)	1	High
Ruby 'Oniguruma-mod' and PHP 'mbstring' forward_search_range Denial of Service (289394)	1	High
Ruby 'Oniguruma-mod' and PHP 'mbstring' parse_char_class Denial of Service (289402)	1	High
Ruby 'Oniguruma-mod' and PHP unicode_unfold_key in 'mbstring' Buffer Overflow (289396)	1	High
Samba '4.x before 4.7.3' Remote Code Execution Vulnerability (297439)	1	High

Samba Remote Code Execution Vulnerability (126509)	1	High
Samba Security Advisory January 2022 (147947)	1	High
SNMP Writeable Communities (104067)	1	High
Unquoted Windows Service Path Vulnerability (117555)	1	High
VMware Security Advisory: VMSA-2015-0007 (121637)	1	High
VMware Security Advisory: VMSA-2018-0026 (126662)	1	High
VMware Security Advisory: VMSA-2019-0012 (129470)	1	High
VMware Security Advisory: VMSA-2019-0022 (131818)	1	High
VMware Security Advisory: VMSA-2020-0023 (142849)	1	High
VMware Security Advisory: VMSA-2020-0026 (143435)	1	High
VMware Security Advisory: VMSA-2021-0002 (144096)	1	High
Web Server Directory Traversal (100905)	1	High
Zend NULL Pointer Denial of Service (278089)	1	High
MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756)	11	Medium
OpenSSH Account Enumeration Vulnerability (126640)	9	Medium
MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133)	8	Medium
NetBIOS Shares Accessible (100870)	8	Medium
OpenSSH 'auth-gss2.c' User Detection Vulnerability (126832)	7	Medium
OpenSSH Missing Character Man-in-The-Middle Attack Vulnerability (127849)	7	Medium
OpenSSH 'Observable Discrepancy' Man-in-the-Middle Vulnerability (137503)	7	Medium
OpenSSH 'scp' Command Evaluation Vulnerability (138013)	7	Medium

OpenSSH scp Server Man-in-The-Middle Attack Vulnerability (127851)	7	Medium
OpenSSH 'stderr' Man-in-The-Middle Attack Vulnerability (127850)	7	Medium
OpenSSH User Enumeration Vulnerability (126863)	7	Medium
OpenSSH Privilege Escalation Vulnerability (146711)	6	Medium
OpenSSH Sensitive Data Exposure Vulnerability (146710)	6	Medium
SMB Writeable Directories (104477)	5	Medium
SNMP Default Communities (100149)	5	Medium
Apache HTTP Server 'httpd' URL Normalization Inconsistency Vulnerability (128448)	4	Medium
Apache HTTP Server 'mod_auth_digest' Access Control Bypass Vulnerability (128444)	4	Medium
Apache HTTP Server 'mod_cache_socache' Out of Bound Read Denial of Service Vulnerability (126242)	4	Medium
Apache HTTP Server 'mod_proxy' Cross-Site Scripting Vulnerability (129590)	4	Medium
Apache HTTP Server 'mod_rewrite' Redirect Vulnerability (133604)	4	Medium
Apache HTTP Server 'mod_session_cookie' Expiry Time Ignored Vulnerability (126276)	4	Medium
Apache HTTP Server Multiple Vulnerabilities (126218)	4	Medium
Apache HTTP Server URL Redirect Vulnerability (129591)	4	Medium
Apache HTTP Server Security Update 2.4.49 (146396)	3	Medium
Java Debugging Port Accessible (104527)	3	Medium
MS09-001 SMB Remote Code Execution (Network Check) (103879)	3	Medium
MS11-020: SMB Transaction Parsing Vulnerability (Network Check) (104422)	3	Medium
MS17-JUN: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128597)	3	Medium

MS17-SEP: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128598)	3	Medium
SSH Accepts Any Login (104178)	3	Medium
Threat Scan: Unsigned Software Processes (127839)	3	Medium
Threat Scan: Windows Defender Definitions Outdated (126741)	3	Medium
Apache httpd Digest Authorization Denial of Service (291127)	2	Medium
Apache HTTP 'HTTP/2 mod' Denial of Service Vulnerability (137993)	2	Medium
Apache HTTP "RequestHeader unset" Directive Bypass Vulnerability (126217)	2	Medium
Apache HTTP Server 'ap_some_auth_required' Function Remote Access Restrictions Bypass Vulnerability (273795)	2	Medium
Apache HTTP Server 'Cache-Digest' Denial of Service Vulnerability (137995)	2	Medium
Apache HTTP Server 'cache_merge_headers_out' Function Denial of Service Vulnerability (126230)	2	Medium
Apache HTTP Server Crafted Request Denial of Service Vulnerability (127001)	2	Medium
Apache HTTP Server 'deflate_in_filter' Function Denial of Service (265521)	2	Medium
Apache HTTP Server Digest Authentication Denial of Service (288580)	2	Medium
Apache HTTP Server HTTP/2 Connections Crafted Request Denial of Service Vulnerability (908009)	2	Medium
Apache HTTP Server HTTP Chunked Request Smuggling Attack (126232)	2	Medium
Apache HTTP Server HTTP_PROXY Environment Variable Vulnerability (126237)	2	Medium
Apache HTTP Server 'lua_websocket_read' Function Denial of Service Vulnerability (126231)	2	Medium
Apache HTTP Server 'mod_cgid' Module Denial of Service (265538)	2	Medium
Apache HTTP Server 'mod_dav' Denial of Service (263007)	2	Medium

Apache HTTP Server 'mod_http2' Memory Corruption Vulnerability (129588)	2	Medium
Apache HTTP Server 'mod_http2' Module Denial of Service Vulnerability (282886)	2	Medium
Apache HTTP Server 'mod_http2' Read-After-Free (CVE-2019-0196) (128447)	2	Medium
Apache HTTP Server 'mod_http2' Read-After-Free (CVE-2019-10082) (129592)	2	Medium
Apache HTTP Server ' mod_log_config' Denial of Service (263002)	2	Medium
Apache HTTP Server 'mod_lua' Access Restriction Bypass Vulnerability (269848)	2	Medium
Apache HTTP Server 'mod_proxy' Module Denial of Service (265530)	2	Medium
Apache HTTP Server 'mod_status' Module Race Condition (265518)	2	Medium
Apache HTTP Server 'mod_userdir' CRLF Injection Vulnerability (126838)	2	Medium
Apache HTTP Server Padding Oracle Vulnerability (288579)	2	Medium
Apache HTTP Server Response Splitting Vulnerability (288581)	2	Medium
Apache HTTP Server 'SETTINGS' Denial of Service Vulnerability (126966)	2	Medium
Apache HTTP Server Slow Request Bodies Denial of Service Vulnerability (126273)	2	Medium
Apache HTTP Server winnt_accept Function Denial of Service (265505)	2	Medium
Apache 'Optionsbleed' UAF Memory Leak (122625)	2	Medium
jQuery Ajax Cross-Site Scripting Vulnerability (126532)	2	Medium
jQuery Cross-Site Scripting Vulnerability (137374)	2	Medium
jQuery Cross-Site Scripting Vulnerability (144402)	2	Medium
MS14-085: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (117082)	2	Medium

MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (117227)	2	Medium
MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (117225)	2	Medium
MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege (117224)	2	Medium
MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass (117223)	2	Medium
MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass (117222)	2	Medium
MS15-007: Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service (117221)	2	Medium
MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass (117376)	2	Medium
MS15-015: Vulnerability in Microsoft Windows Could Allow Elevation of Privilege (117375)	2	Medium
MS15-016: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (117374)	2	Medium
MS15-023: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (117474)	2	Medium
MS15-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (117472)	2	Medium
MS15-027: Vulnerability in NETLOGON Could Allow Spoofing (117470)	2	Medium
MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (117469)	2	Medium
MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (117468)	2	Medium
MS15-030: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (117467)	2	Medium
MS15-031: Vulnerability in Schannel Could Allow Security Feature Bypass (117466)	2	Medium
MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (117582)	2	Medium

MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure (117579)	2	Medium
MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (117733)	2	Medium
MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege (117731)	2	Medium
MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (117730)	2	Medium
MS15-052: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (117729)	2	Medium
MS15-055: Vulnerability in Schannel Could Allow Information Disclosure (117726)	2	Medium
MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution (117875)	2	Medium
MS15-061: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (117874)	2	Medium
MS15-071: Vulnerability in Netlogon Could Allow Elevation of Privilege (118044)	2	Medium
MS15-072: Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (118043)	2	Medium
MS15-073: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (118042)	2	Medium
MS15-075: Vulnerabilities in OLE Could Allow Elevation of Privilege (118040)	2	Medium
MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (118039)	2	Medium
MS15-077: Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (118038)	2	Medium
MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution (118131)	2	Medium
MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure (118129)	2	Medium

MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege (118128)	2	Medium
MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure (118125)	2	Medium
MS15-092: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (118121)	2	Medium
MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (118251)	2	Medium
MS15-119: Security Update for Winsock to Address Elevation of Privilege (118492)	2	Medium
MS15-120: Security Update for IPSec to Address Denial of Service (118491)	2	Medium
MS15-121: Security Update for Schannel to Address Spoofing (118490)	2	Medium
MS15-122: Security Update for Kerberos to Address Security Feature Bypass (118489)	2	Medium
MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (118662)	2	Medium
MS15-133: Security Update for Windows PGM to Address Elevation of Privilege (118661)	2	Medium
MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (118683)	2	Medium
MS16-008: Security Update for Windows Kernel to Address Elevation of Privilege (118682)	2	Medium
MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (118982)	2	Medium
MS16-018: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (118978)	2	Medium
MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service (118975)	2	Medium
MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (119085)	2	Medium
MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (119084)	2	Medium

MS16-034: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (119083)	2	Medium
MS16-048: Security Update for CSRSS (119268)	2	Medium
MS16-060: Security Update for Windows Kernel (119357)	2	Medium
MS16-061: Security Update for Microsoft RPC (119356)	2	Medium
MS16-065: Security Update for .NET Framework (119353)	2	Medium
MS16-072: Security Update for Group Policy (119500)	2	Medium
MS16-073: Security Update for Windows Kernel-Mode Drivers (119499)	2	Medium
MS16-074: Security Update for Microsoft Graphics Component (119498)	2	Medium
MS16-075: Security Update for Windows SMB Server (119497)	2	Medium
MS16-076: Security Update for Netlogon (119496)	2	Medium
MS16-077: Security Update for WPAD (119495)	2	Medium
MS16-080: Security Update for Microsoft Windows PDF (119492)	2	Medium
MS16-082: Security Update for Microsoft Windows Search Component (119490)	2	Medium
MS16-090: Security Update for Windows Kernel-Mode Drivers (119627)	2	Medium
MS16-092: Security Update for Windows Kernel (119625)	2	Medium
MS16-111: Security Update for Windows Kernel (120911)	2	Medium
MS16-112: Security Update for Windows Lock Screen (120910)	2	Medium
MS16-114: Security Update for Windows SMBv1 Server (120908)	2	Medium
MS16-134: Security Update for Common Log File System Driver (121128)	2	Medium
MS16-135: Security Update for Windows Kernel-Mode Drivers (121127)	2	Medium
MS16-138: Security Update to Microsoft Virtual Hard Drive (121124)	2	Medium

MS16-149: Security Update for Windows (121322)	2	Medium
MS16-151: Security Update for Kernel-Mode Driver (121320)	2	Medium
MS16-153: Security Update for Common Log File System Driver (121318)	2	Medium
MS17-016: Security Update for Windows IIS (121900)	2	Medium
MS17-017: Security Update for Windows Kernel (121899)	2	Medium
MS17-018: Security Update for Windows Kernel-Mode Drivers (121898)	2	Medium
MS17-021: Security Update for Windows DirectShow (121895)	2	Medium
MS17-022: Security Update for Microsoft XML Core Services (121894)	2	Medium
MS17-AUG: Microsoft Internet Explorer Security Update (122396)	2	Medium
MS17-JUN: Microsoft Internet Explorer Security Update (122280)	2	Medium
MS17-MAY: Microsoft .NET Security Update (122158)	2	Medium
MS17-NOV: Microsoft Windows Security Update (122792)	2	Medium
MS18-JAN: Microsoft .NET Security Update (123656)	2	Medium
MS18-JAN: Microsoft Windows Security Update (MELTDOWN) (123603)	2	Medium
MS18-JUL: Microsoft .NET Security Update (125658)	2	Medium
MS18-MAY: Microsoft .NET Security Update (124370)	2	Medium
MS18-NOV: Microsoft Internet Explorer Security Update (126948)	2	Medium
MS19-JAN: Microsoft Internet Explorer Security Update (127738)	2	Medium
MS19-MAY: Microsoft .NET Security Update (128800)	2	Medium
MS21-JAN: Microsoft SQL Server Security Update (143780)	2	Medium
OpenSSH 'before 7.6' 'process_open function in sftp-server.c' subcomponent Does not Properly Prevent Write Operations in Readonly Mode Vulnerability (296108)	2	Medium

OpenSSH BLOWFISH Hashing User Enumeration (280859)	2	Medium
OpenSSH kex.c and packet.c NULL Pointer Dereference Denial of Service (299655)	2	Medium
OpenSSH Privilege Escalation Vulnerability (126645)	2	Medium
Threat Scan: Antivirus Software Not Installed (126539)	2	Medium
Threat Scan: Windows Defender Disabled (127063)	2	Medium
Heimdal Man-in-the-Middle Vulnerability (291123)	1	Medium
LDAP Channel Binding Vulnerability (132377)	1	Medium
LDAP Signing Vulnerability (129050)	1	Medium
libxml 'libxml_disable_entity_loader' XXE and XEE Vulnerability (278493)	1	Medium
MS18-JAN: Microsoft Windows Security Update - Registry Entry Not Set (128655)	1	Medium
MS18-NOV: Microsoft Windows Security Update - Registry Entry Not Set (128666)	1	Medium
MS19-MAY: Microsoft Windows Security Update (ZombieLoad) - Registry Entry Not Set (128823)	1	Medium
MS19-NOV: Microsoft Windows Security Update - Registry Entry Not Set (131738)	1	Medium
OpenSSH Heap-Based Buffer Overflow Vulnerability (126642)	1	Medium
OpenSSH Information Disclosure Vulnerability (126643)	1	Medium
OpenSSH monitor.c 'mm_answer_pam_free_ctx' Use-After-Free Vulnerability (126919)	1	Medium
OpenSSH Remote Command Injection Vulnerability (126646)	1	Medium
OpenSSH 'ssh_packet_read_poll2' Function Denial of Service (275984)	1	Medium
OpenSSH 'x11_open_helper' Function Access Restriction Bypass (273896)	1	Medium

OpenSSL Deprecated Function 'RAND_pseudo_bytes' (278298)	1	Medium
PHP 5.6.x and 7.x 'gdImageRotateInterpolated' Function Denial of Service (275989)	1	Medium
PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 Remote Denial of Service Vulnerability (280831)	1	Medium
PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3: Metadata can be set by an attacker (900437)	1	Medium
PHP 'before 5.6.32, 7.x before 7.0.25, 7.1.x before 7.1.11' Interpreter Information Leak Vulnerability (296552)	1	Medium
PHP 'Bucket Brigade' Vulnerability (126955)	1	Medium
PHP bz2.c 'bzread' Denial of Service (280832)	1	Medium
PHP 'cdf_check_stream_offset' Function Denial of Service (265280)	1	Medium
PHP cdf.c Integer Overflow Denial of Service (266029)	1	Medium
PHP 'cdf_count_chain' Function Denial of Service (265272)	1	Medium
PHP 'cdf_read_property_info' Function Denial of Service (265277)	1	Medium
PHP 'cdf_read_property_info' in Fileinfo Component Denial of Service (264496)	1	Medium
PHP 'cdf_unpack_summary_info' in Fileinfo Component Denial of Service (264495)	1	Medium
PHP 'data_len' Uninitialized Read Vulnerability (128705)	1	Medium
PHP dirstream.c 'phar_make_dirstream' Mishandled Zero-size Denial of Service (277156)	1	Medium
PHP dns.c 'php_parserr' Function Buffer Overflow Denial of Service (266027)	1	Medium
PHP 'do_soap_call' Function Type Confusion Vulnerability (272828)	1	Medium
PHP exif.c 'exif_convert_any_to_int' Denial of Service (284033)	1	Medium
PHP exif.c 'exif_process_IFD_in_TIFF' Information Disclosure (281189)	1	Medium
PHP 'exif.c' Integer Overflow Vulnerability (126957)	1	Medium

PHP 'exif.c' Out-of-Bounds Read Vulnerability (126960)	1	Medium
PHP 'EXIF' Extension Crafted JPEG Denial of Service (268715)	1	Medium
PHP 'exif_process_SOFn' Invalid Read Vulnerability (128706)	1	Medium
PHP 'exif_process_unicode' Function EXIF Data Denial of Service Flaw (270518)	1	Medium
PHP 'exif_process_user_comment' Denial of Service (277618)	1	Medium
PHP 'ext/iconv/iconv.c' Infinite Loop Vulnerability (126961)	1	Medium
PHP 'ext/ldap/ldap.c' Denial of Service Vulnerability (126962)	1	Medium
PHP 'ext/phar/phar.c' Buffer Over-read Vulnerability (272068)	1	Medium
PHP 'ext/phar/phar_object.c' Cross-site Scripting Vulnerability (126963)	1	Medium
PHP 'ext/spl/spl_array.c' Denial of Service Vulnerability (127032)	1	Medium
PHP 'ext/spl/spl_dllist.c' Denial of Service Vulnerability (127031)	1	Medium
PHP Fileinfo Component Denial of Service (265273)	1	Medium
PHP 'Fileinfo' Component Denial of Service Vulnerability (127024)	1	Medium
PHP Fileinfo Component Pascal String Denial of Service Flaw (271045)	1	Medium
PHP 'fsockopen' Server-Side Request Forgery Vulnerability (286727)	1	Medium
PHP '_gd2GetHeader' Denial of Service Vulnerability (127021)	1	Medium
PHP 'gd.c' Denial of Service Vulnerability (126992)	1	Medium
PHP 'gd_crop.c' Denial of Service Vulnerability (126980)	1	Medium
PHP gd_ctx.c Arbitrary File Overwrite Vulnerabilty (266023)	1	Medium
PHP gd_gif_in.c Crafted GIF Denial of Service (299341)	1	Medium
PHP gd_gif_in.c 'gdImageCreateFromGifCtx' Information Disclosure (291957)	1	Medium

PHP 'gdImageCreate' Denial of Service Vulnerability (127022)	1	Medium
PHP 'gd_interpolation.c' Denial of Service Vulnerability (127028)	1	Medium
PHP gd_interpolation.c 'gdImageScaleTwoPass' Denial of Service (277173)	1	Medium
PHP 'GetCode_' Function Crafted GIF Image Denial of Service (271572)	1	Medium
PHP GMP Interfaces Denial of Service (287844)	1	Medium
PHP HTTP_PROXY Environment Variable Namespace Conflict (279443)	1	Medium
PHP 'imagefilltoborder' Denial of Service (277172)	1	Medium
PHP JPEG Denial of Service Vulnerability (126958)	1	Medium
PHP 'linkinfo' File Path Disclosure Vulnerability (126959)	1	Medium
PHP "main/php_open_temporary_file.c" Thread Safety Denial of Service Flaw (278227)	1	Medium
PHP 'make_http_soap_request' Function Denial of Service (276913)	1	Medium
PHP 'mconvert' Function Denial of Service (265276)	1	Medium
PHP 'mcopy' Function Fileinfo Component Denial of Service (273417)	1	Medium
PHP 'mget' Function Fileinfo Component Denial of Service (273416)	1	Medium
PHP 'mod_php' Or 'php-fpm' Information Disclosure (285650)	1	Medium
PHP 'move_uploaded_file' Extension Restrictions Bypass Flaw (271565)	1	Medium
PHP msgformat_format.c 'MessageFormatter::formatMessage' Denial of Service Vulnerability (281200)	1	Medium
PHP 'multipart_buffer_headers' Function Algorithmic Complexity Vulnerability (272827)	1	Medium
PHP Multiple Pathname Sanitization Remote Arbitrary File Access Vulnerabilities (273408)	1	Medium

PHP mysqlnd Man in the Middle via Cleartext-downgrade (276914)	1	Medium
PHP mysqlnd_wireprotocol.c BIT Field Heap Buffer Overflow (281198)	1	Medium
PHP Non-Blocking STDIN Stream Denial of Service Vulnerability (127023)	1	Medium
PHP "odbc_bindcols" Function Denial of Service Flaw (278354)	1	Medium
PHP openssl.c Denial of Service (290992)	1	Medium
PHP parse_date.c 'php_parse_date' Information Disclosure (290999)	1	Medium
PHP PHAR 404 Error Page Reflected Cross-Site Scripting (299348)	1	Medium
PHP phar.c 'phar_parse_pharfile' Denial of Service (284031)	1	Medium
PHP phar.c 'phar_parse_pharfile' Denial of Service (290980)	1	Medium
PHP PharData 'extractTo' Directory Traversal (275417)	1	Medium
PHP 'phar_parse_tarfile' Function Denial of Service (272802)	1	Medium
PHP 'php_handler' Function Denial of Service (272066)	1	Medium
PHP 'php_imap.c' Denial of Service Vulnerability (126280)	1	Medium
PHP 'php_raw_url_encode' Denial of Service (277151)	1	Medium
PHP 'php_stream_zip_opener' Stack Buffer Overflow (277625)	1	Medium
PHP php_variables.c Denial of Service (291000)	1	Medium
PHP PostgreSQL 'build_tablename' Function Denial of Service Flaw (271047)	1	Medium
PHP PostgreSQL Extension 'php_pgsql_meta_data' Function Denial of Service (273432)	1	Medium
PHP 'rename()' Sensitive Data Disclosure Vulnerability (128703)	1	Medium
PHP 'sapi_header_op' Function Cross-Site Scripting Vulnerability (280826)	1	Medium
PHP session.c Invalid Session Names Object Injection (281187)	1	Medium

PHP 'stream_resolve_include_path ' Function Pathname Sanitization Remote Arbitrary File Access Vulnerability (273409)	1	Medium
PHP url.c 'parse_url' Restriction Bypass (290996)	1	Medium
PHP util.c 'phar_get_entry_data' Denial of Service (275603)	1	Medium
PHP 'value_len' Uninitialized Read Vulnerability (128704)	1	Medium
PHP 'var_unserializer.c' Denial of Service Vulnerability (126256)	1	Medium
PHP var_unserializer.c 'object_common1' Denial of Service (284032)	1	Medium
PHP 'virtual_file_ex' Stack Buffer Overflow (277731)	1	Medium
PHP 'wddx.c' PDORow String Denial of Service (283445)	1	Medium
PHP wddx.c 'php_wddx_pop_element' NULL Pointer Dereference Denial of Service Vulnerability (281191)	1	Medium
PHP wddx.c 'php_wddx_push_element' Denial of Service (281202)	1	Medium
PHP wddx.c 'wddx_deserialize' NULL Pointer Dereference Denial of Service Vulnerability (281193)	1	Medium
PHP wddx.c 'wddx_deserialize' NULL Pointer Dereference Denial of Service Vulnerability (281192)	1	Medium
PHP wddx.c XML Deserialization Denial of Service (290987)	1	Medium
PHP WSDL Injection Attack Vulnerability (127026)	1	Medium
PHP 'xmlrpc_decode()' Memory Over-Read Vulnerability (127912)	1	Medium
PHP XMLRPC Extension Denial of Service (268706)	1	Medium
PHP xsltprocessor.c 'xsl_ext_function_php' Denial of Service During Initial Error Checking (275419)	1	Medium
PHP xsltprocessor.c 'xsl_ext_function_php' Denial of Service During Principal Argument Loop (275420)	1	Medium
PHP Zend Denial of Service Vulnerability (126972)	1	Medium
PHP zend_exceptions.c Crafted Exception Object Denial of Service (283558)	1	Medium

PHP 'ZipArchive::extractTo' Function Directory Traversal (276911)	1	Medium
PHP zip.c 'phar_parse_zipfile' Denial of Service (275604)	1	Medium
Ruby 'Oniguruma-mod' and PHP 'mbstring' forward_search_range Denial of Service (289404)	1	Medium
Samba 'before 4.7.3' Possible Remote Sensitive Information Access Vulnerability (297423)	1	Medium
Samba Confidential Attribute Values Disclosure Vulnerability (126516)	1	Medium
Samba 'DelegationNotAllowed' Vulnerability (131863)	1	Medium
Samba 'dirsync' Denial of Service Vulnerability (131712)	1	Medium
Samba 'DNS' Denial of Service Vulnerability (131862)	1	Medium
Samba Incorrect 'KDC' Implementation Vulnerability (129055)	1	Medium
Samba Input Validation Vulnerability (126518)	1	Medium
Samba 'KDC' Denial of Service Vulnerability (127055)	1	Medium
Samba Kerberos Impersonation Vulnerability (126871)	1	Medium
Samba 'LDAP' Search Denial of Service Vulnerability (126956)	1	Medium
Samba 'LDAP' Server Denial of Service Vulnerability (126834)	1	Medium
Samba Man in the Middle Hijack Vulnerability (126512)	1	Medium
Samba Man in the Middle Vulnerability (126511)	1	Medium
Samba 'ndr_pull_dnsp_name' Remote Privilege Escalation Vulnerability (126870)	1	Medium
Samba November 2021 Security Update (146961)	1	Medium
Samba 'PAC' Checksum Denial of Service Vulnerability (126872)	1	Medium
Samba Password Change Vulnerability (126513)	1	Medium
Samba Registry Hive File Creation Vulnerability (128710)	1	Medium

Samba Server Memory Information Leak over SMB1 (126510)	1	Medium
Samba 'smbXcli_base.c' Man-In-The-Middle Client-Signing Protection Bypass (277364)	1	Medium
Samba Symlink Denial of Service (289653)	1	Medium
Samba Unauthorized File Creation Vulnerability (131710)	1	Medium
Slowloris Resource Depletion And Denial Of Service (104012)	1	Medium
Threat Scan: McAfee VirusScan Enterprise Definitions Outdated (126543)	1	Medium
Threat Scan: McAfee VirusScan Enterprise Disabled (127060)	1	Medium
VMware Security Advisory: VMSA-2018-0012 (126058)	1	Medium
VMware Security Advisory: VMSA-2018-0016 (127203)	1	Medium
VMware Security Advisory: VMSA-2018-0018 (126661)	1	Medium
VMware Security Advisory: VMSA-2018-0020 (126059)	1	Medium
VMware Security Advisory: VMSA-2019-0006 (129035)	1	Medium
VMware Security Advisory: VMSA-2019-0008 (129335)	1	Medium
VMware Security Advisory: VMSA-2019-0013 (129784)	1	Medium
VMware Security Advisory: VMSA-2019-0020 (131817)	1	Medium
VMware Security Advisory: VMSA-2020-0008 (137342)	1	Medium
VMware Security Advisory: VMSA-2020-0012 (137344)	1	Medium
VMware Security Advisory: VMSA-2020-0015 (137463)	1	Medium
VMware Security Advisory: VMSA-2020-0018 (138134)	1	Medium
VMware Security Advisory: VMSA-2021-0014 (148212)	1	Medium
VMware Security Advisory: VMSA-2022-0001 (148215)	1	Medium

VMware Security Advisory: VMSA-2022-0004 (148216)	1	Medium
Zend Recursive Method Denial of Service (278791)	1	Medium
Zoom 'Share Screen' Information Disclosure Vulnerability (144747)	1	Medium
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)	59	Low
SMB Security Signatures Not Required (104188)	47	Low
SSL Connection: SSL Version 3 Enabled (128440)	33	Low
PHP End of Life (112906)	18	Low
Web Server Directory Indexing Enabled (101049)	17	Low
ISC BIND End Of Life (123915)	14	Low
Product Has Reached End-of-Life Status (104220)	14	Low
HTTP Host Header Value Reflection (128596)	13	Low
SMB User Enumeration (113348)	12	Low
Anonymous FTP Enabled (101362)	11	Low
Phpinfo.php System Information Disclosure (100403)	11	Low
SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843)	11	Low
Slowloris Resource Depletion And Denial Of Service (117854)	10	Low
Debian End of Life (134009)	9	Low
Apache Default Start Page (103388)	7	Low
OpenSSH scp Client Access Bypass Vulnerability (127848)	7	Low
Protocol Allows Authentication Over Clear Text (104798)	7	Low
Samba End of Life (117557)	7	Low
Ubuntu End of Life (117365)	7	Low

Apache Manual Page Information Leak (103390)	6	Low
SSL Connection: Server Appears Vulnerable to ChangeCipherSpec Injection (115134)	6	Low
Microsoft Windows Service Pack Outdated (104065)	5	Low
NetBIOS Shares With Everyone/Full-Control Permissions (104589)	5	Low
OpenSSH Security Advisory (148395)	5	Low
SSL Connection: RSA Export Grade Cipher FREAK Vulnerability (117845)	5	Low
SSL Connection: TLS Diffie-Hellman Export Cipher Downgrade Logjam Vulnerability (117846)	5	Low
Apache Username Disclosure (101469)	4	Low
SMTP Server EXPN/VRFY (100876)	4	Low
Apache Range Header Denial Of Service (117860)	3	Low
Apache Tomcat End of Life (113012)	3	Low
Insecure Crossdomain.xml Directives (104181)	3	Low
MS09-048 Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities (104048)	3	Low
OpenSSL AES-NI CBC Padding Oracle Attack (119367)	3	Low
Webserver Expect Header Allows Cross-Site Scripting (104910)	3	Low
Apache HTTP Server mod_cluster Improper Input Validation Vulnerability (126238)	2	Low
OpenSSH Local Information Disclosure Vulnerability (126644)	2	Low
OpenSSL End of Life (123917)	2	Low
WordPress Unsupported Version (128586)	2	Low
FreeBSD End of Life (117558)	1	Low
HTTP XML Injection (104276)	1	Low

Insecure HTML5 Cross Origin Request Policy (118119)	1	Low
MS22-MAY: Microsoft .NET Security Update (148574)	1	Low
OpenSSH 'sshd' Monitor Component Local Impersonation Vulnerability (274384)	1	Low
PHP 'ext/standard/info.c' Sensitive Information Disclosure (127033)	1	Low
PHP 'gdImageColorMatch' Buffer Overflow Vulnerability (127853)	1	Low
PHP PEAR REST Arbitrary File Write Vulnerability (127016)	1	Low
PHP 'PHP-FPM' Information Disclosure Vulnerability (126964)	1	Low
PHP '/tmp/phpglibccheck' File Overwrite Vulnerability (127030)	1	Low
Quote Of The Day Service (100935)	1	Low
SSH Protocol 1 Enabled (100561)	1	Low
VMware Security Advisory: VMSA-2018-0027 (127205)	1	Low
VMware Security Advisory: VMSA-2019-0005 (128528)	1	Low
VMware Security Advisory: VMSA-2019-0014 (129785)	1	Low
VMware Security Advisory: VMSA-2019-0019 (131816)	1	Low
VMware Security Advisory: VMSA-2020-0011 (137343)	1	Low
VMware Security Advisory: VMSA-2022-0016 (149533)	1	Low
VMware Security Advisory: VMSA-2022-0020 (149535)	1	Low
VNC Weak Password Encryption (101410)	1	Low
Web Server Uses Unencrypted/Plaintext Form Password Fields (103980)	1	Low
TLS Connection: TLS Version 1.0 Enabled (125641)	86	Trivial
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)	84	Trivial
SSL Connection: Sweet32 Vulnerability (121110)	76	Trivial

SMB Native LanMan Version (100092)	65	Trivial
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)	59	Trivial
TLS Connection: TLS Version 1.1 Enabled (145426)	57	Trivial
Web Server Default Error Page Detected (128223)	44	Trivial
SMB Null Session Authentication (101373)	39	Trivial
SSL Certificate: Weak Signature Algorithm SHA-1 (121119)	37	Trivial
Content Security Policy Missing (148043)	34	Trivial
Apache Server Header Information Disclosure (123916)	12	Trivial
Remote Desktop Protocol Allows Man in the Middle (117858)	12	Trivial
RPC Portmap Service (100505)	10	Trivial
SSL Certificate: Outdated Version (104020)	10	Trivial
IPv6 Enabled (142306)	9	Trivial
SSL Certificate: Expired Certificate Date (103615)	9	Trivial
Default IIS Webpage Detected (117366)	8	Trivial
HTTP TRACE/TRACK Method Enabled (117856)	8	Trivial
Link Local Multicast Name Resolution (LLMNR) Enabled (129962)	8	Trivial
SSL Connection: TLS Compression Enabled (112280)	8	Trivial
Compliance: Configure 'Accounts: Rename administrator account' (120563)	7	Trivial
Compliance: Configure 'Accounts: Rename guest account' (120564)	7	Trivial
Compliance: Configure 'Create symbolic links' (120536)	7	Trivial
Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (120581)	7	Trivial

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (120582)	7	Trivial
Compliance: Configure 'Manage auditing and security log' (120548)	7	Trivial
Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (120525)	7	Trivial
Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (120522)	7	Trivial
Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (120523)	7	Trivial
Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (120559)	7	Trivial
Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (120560)	7	Trivial
Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (120561)	7	Trivial
Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (120562)	7	Trivial
Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (120526)	7	Trivial
Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (120528)	7	Trivial
Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120809)	7	Trivial
Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120806)	7	Trivial
Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (120790)	7	Trivial
Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (120749)	7	Trivial
Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120807)	7	Trivial
Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120810)	7	Trivial

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (120800)	7	Trivial
Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120825)	7	Trivial
Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120801)	7	Trivial
Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (120782)	7	Trivial
Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120763)	7	Trivial
Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120764)	7	Trivial
Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (120712)	7	Trivial
Compliance: Ensure 'Audit Account Lockout' is set to 'Success' (120667)	7	Trivial
Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (120658)	7	Trivial
Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (120673)	7	Trivial
Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (120674)	7	Trivial
Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (120659)	7	Trivial
Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (120657)	7	Trivial
Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (120565)	7	Trivial
Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (120676)	7	Trivial
Compliance: Ensure 'Audit Logoff' is set to 'Success' (120668)	7	Trivial

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (120669)	7	Trivial
Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (120661)	7	Trivial
Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (120670)	7	Trivial
Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (120677)	7	Trivial
Compliance: Ensure 'Audit Process Creation' is set to 'Success' (120664)	7	Trivial
Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (120672)	7	Trivial
Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (120662)	7	Trivial
Compliance: Ensure 'Audit Security State Change' is set to 'Success' (120678)	7	Trivial
Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (120679)	7	Trivial
Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (120675)	7	Trivial
Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (120566)	7	Trivial
Compliance: Ensure 'Audit Special Logon' is set to 'Success' (120671)	7	Trivial
Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (120680)	7	Trivial
Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (120663)	7	Trivial
Compliance: Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (120799)	7	Trivial
Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (120529)	7	Trivial
Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (120715)	7	Trivial

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (120530)	7	Trivial
Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (120531)	7	Trivial
Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (120813)	7	Trivial
Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (120814)	7	Trivial
Compliance: Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (120798)	7	Trivial
Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (120741)	7	Trivial
Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (120716)	7	Trivial
Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (120717)	7	Trivial
Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (120742)	7	Trivial
Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' (120771)	7	Trivial
Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (120532)	7	Trivial
Compliance: Ensure 'Create a token object' is set to 'No One' (120533)	7	Trivial
Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (120534)	7	Trivial
Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (120535)	7	Trivial
Compliance: Ensure 'Debug programs' is set to 'Administrators' (120537)	7	Trivial
Compliance: Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (120756)	7	Trivial

Compliance: Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (120757)	7	Trivial
Compliance: Ensure 'Default Protections for Popular Software' is set to 'Enabled' (120758)	7	Trivial
Compliance: Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (120759)	7	Trivial
Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (120538)	7	Trivial
Compliance: Ensure 'Deny log on as a service' to include 'Guests' (120539)	7	Trivial
Compliance: Ensure 'Deny log on locally' to include 'Guests' (120540)	7	Trivial
Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (120541)	7	Trivial
Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (120567)	7	Trivial
Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (120568)	7	Trivial
Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (120750)	7	Trivial
Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (120808)	7	Trivial
Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (120811)	7	Trivial
Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (120572)	7	Trivial
Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (120573)	7	Trivial
Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (120574)	7	Trivial
Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (120575)	7	Trivial
Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (120576)	7	Trivial

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (120577)	7	Trivial
Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (120779)	7	Trivial
Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (120684)	7	Trivial
Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (120776)	7	Trivial
Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (120787)	7	Trivial
Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (120734)	7	Trivial
Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (120753)	7	Trivial
Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (120735)	7	Trivial
Compliance: Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (120822)	7	Trivial
Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (120788)	7	Trivial
Compliance: Ensure 'EMET 5.5' or higher is installed (120755)	7	Trivial
Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (120685)	7	Trivial
Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (120743)	7	Trivial
Compliance: Ensure 'Enable screen saver' is set to 'Enabled' (120816)	7	Trivial
Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (120516)	7	Trivial
Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (120754)	7	Trivial
Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (120736)	7	Trivial

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (120542)	7	Trivial
Compliance: Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (120817)	7	Trivial
Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120543)	7	Trivial
Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (120706)	7	Trivial
Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (120714)	7	Trivial
Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (120544)	7	Trivial
Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (120578)	7	Trivial
Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (120579)	7	Trivial
Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (120580)	7	Trivial
Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (120584)	7	Trivial
Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (120585)	7	Trivial
Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (120586)	7	Trivial
Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (120683)	7	Trivial
Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (120545)	7	Trivial
Compliance: Ensure 'Lock pages in memory' is set to 'No One' (120546)	7	Trivial
Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (120517)	7	Trivial

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (120587)	7	Trivial
Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (120588)	7	Trivial
Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (120589)	7	Trivial
Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (120590)	7	Trivial
Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (120591)	7	Trivial
Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (120592)	7	Trivial
Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (120593)	7	Trivial
Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (120594)	7	Trivial
Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (120710)	7	Trivial
Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (120518)	7	Trivial
Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (120519)	7	Trivial
Compliance: Ensure 'Modify an object label' is set to 'No One' (120549)	7	Trivial
Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (120550)	7	Trivial
Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (120689)	7	Trivial
Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disa... (120691)	7	Trivial

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely... (120690)	7	Trivial
Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (120692)	7	Trivial
Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (120694)	7	Trivial
Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (120696)	7	Trivial
Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (120697)	7	Trivial
Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (120700)	7	Trivial
Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (120595)	7	Trivial
Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (120597)	7	Trivial
Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (120596)	7	Trivial
Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (120599)	7	Trivial
Compliance: Ensure 'Network access: Remotely accessible registry paths' (120600)	7	Trivial
Compliance: Ensure 'Network access: Remotely accessible registry paths and sub-paths' (120601)	7	Trivial
Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (120602)	7	Trivial
Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (120603)	7	Trivial
Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (120604)	7	Trivial

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (120606)	7	Trivial
Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (120605)	7	Trivial
Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (120607)	7	Trivial
Compliance: Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (120608)	7	Trivial
Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (120609)	7	Trivial
Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (120610)	7	Trivial
Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (120611)	7	Trivial
Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (120612)	7	Trivial
Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120613)	7	Trivial
Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120614)	7	Trivial
Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (120815)	7	Trivial
Compliance: Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (120823)	7	Trivial
Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (120520)	7	Trivial
Compliance: Ensure 'Password protect the screen saver' is set to 'Enabled' (120818)	7	Trivial

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (120688)	7	Trivial
Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (120686)	7	Trivial
Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (120687)	7	Trivial
Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (120551)	7	Trivial
Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (120789)	7	Trivial
Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (120681)	7	Trivial
Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (120682)	7	Trivial
Compliance: Ensure 'Prevent the usage of SkyDrive for file storage' is set to 'Enabled' (120792)	7	Trivial
Compliance: Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (120824)	7	Trivial
Compliance: Ensure 'Profile single process' is set to 'Administrators' (120552)	7	Trivial
Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (120553)	7	Trivial
Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (120704)	7	Trivial
Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120554)	7	Trivial
Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (120705)	7	Trivial
Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (120783)	7	Trivial
Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (120524)	7	Trivial

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (120555)	7	Trivial
Compliance: Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (120819)	7	Trivial
Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120765)	7	Trivial
Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (120766)	7	Trivial
Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (120784)	7	Trivial
Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (120751)	7	Trivial
Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120767)	7	Trivial
Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120768)	7	Trivial
Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (120615)	7	Trivial
Compliance: Ensure 'Shut down the system' is set to 'Administrators' (120556)	7	Trivial
Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (120803)	7	Trivial
Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (120521)	7	Trivial
Compliance: Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (120760)	7	Trivial
Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120769)	7	Trivial
Compliance: Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (120761)	7	Trivial
Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (120616)	7	Trivial

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (120617)	7	Trivial
Compliance: Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (120762)	7	Trivial
Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120770)	7	Trivial
Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (120558)	7	Trivial
Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (120737)	7	Trivial
Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (120794)	7	Trivial
Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (120752)	7	Trivial
Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (120718)	7	Trivial
Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (120772)	7	Trivial
Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (120773)	7	Trivial
Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (120774)	7	Trivial
Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (120795)	7	Trivial
Compliance: Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (120820)	7	Trivial
Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (120738)	7	Trivial
Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (120804)	7	Trivial
Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (120805)	7	Trivial

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (120618)	7	Trivial
Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (120619)	7	Trivial
Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (120620)	7	Trivial
Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (120621)	7	Trivial
Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (120622)	7	Trivial
Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (120623)	7	Trivial
Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (120624)	7	Trivial
Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (120625)	7	Trivial
Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (120626)	7	Trivial
Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (120713)	7	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (120627)	7	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (120628)	7	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (120635)	7	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (120636)	7	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewalldomainfw.log' (120633)	7	Trivial

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120634)	7	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (120629)	7	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (120632)	7	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (120631)	7	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (120630)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (120637)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (120638)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (120645)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (120646)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallprivatefw.log' (120643)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120644)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (120639)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (120642)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (120641)	7	Trivial
Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (120640)	7	Trivial
Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (120647)	7	Trivial

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (120648)	7	Trivial
Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (120655)	7	Trivial
Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (120656)	7	Trivial
Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallpublicfw.log' (120653)	7	Trivial
Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120654)	7	Trivial
Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (120649)	7	Trivial
Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (120652)	7	Trivial
Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (120651)	7	Trivial
Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (120650)	7	Trivial
Microsoft RDP Network Level Authentication Disabled (128925)	7	Trivial
SSL Certificate: Chain Contains Weak RSA Keys (104022)	7	Trivial
Default Apache Tomcat Webpage Detected (117554)	6	Trivial
NTLM Authentication Host Information Disclosure (117943)	5	Trivial
SSL Connection: Anonymous (non-authenticated) Key-Agreement Protocols Permitted (122162)	5	Trivial
SSL Connection: Weak Ciphers Enabled (103617)	5	Trivial
TDS SQL Database Service (101436)	5	Trivial
TLS Connection: TLS Version 1.2 Not Enabled (146258)	5	Trivial
Apache ETags Inode Number Disclosure (121914)	4	Trivial
CIS Benchmark Profile (116437)	3	Trivial

Kerberos User Enumeration Detected (138135)	3	Trivial
NetBIOS Over TCP/IP Enabled (124295)	3	Trivial
Apache HTTP Server Denial of Service (902560)	2	Trivial
Compliance: Configure 'Access this computer from the network' (122896)	2	Trivial
Compliance: Configure 'Accounts: Rename administrator account' (122947)	2	Trivial
Compliance: Configure 'Accounts: Rename guest account' (122948)	2	Trivial
Compliance: Configure 'Allow log on locally' (122901)	2	Trivial
Compliance: Configure 'Allow log on through Remote Desktop Services' (122903)	2	Trivial
Compliance: Configure 'Create symbolic links' (122912)	2	Trivial
Compliance: Configure 'Deny access to this computer from the network' (122915)	2	Trivial
Compliance: Configure 'Enable computer and user accounts to be trusted for delegation' (122921)	2	Trivial
Compliance: Configure 'Impersonate a client after authentication' (122925)	2	Trivial
Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (122967)	2	Trivial
Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (122968)	2	Trivial
Compliance: Configure 'Manage auditing and security log' (122931)	2	Trivial
Compliance: Configure 'Network access: Named Pipes that can be accessed anonymously' (122988)	2	Trivial
Compliance: Configure 'Network access: Remotely accessible registry paths' (122990)	2	Trivial
Compliance: Configure 'Network access: Remotely accessible registry paths and sub-paths' (122991)	2	Trivial

Compliance: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (123114)	2	Trivial
Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (122895)	2	Trivial
Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (122891)	2	Trivial
Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (122892)	2	Trivial
Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (122943)	2	Trivial
Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (122944)	2	Trivial
Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (122945)	2	Trivial
Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (122946)	2	Trivial
Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (122898)	2	Trivial
Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (122900)	2	Trivial
Compliance: Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (123168)	2	Trivial
Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (123246)	2	Trivial
Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (123249)	2	Trivial
Compliance: Ensure 'Allow Cortana above lock screen' is set to 'Disabled' (123226)	2	Trivial
Compliance: Ensure 'Allow Cortana' is set to 'Disabled' (123225)	2	Trivial
Compliance: Ensure 'Allow Extensions' is set to 'Disabled' (123198)	2	Trivial
Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (123227)	2	Trivial

Compliance: Ensure 'Allow InPrivate Browsing' is set to 'Disabled' (123199)	2	Trivial
Compliance: Ensure 'Allow Input Personalization' is set to 'Disabled' (123077)	2	Trivial
Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (123170)	2	Trivial
Compliance: Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (123155)	2	Trivial
Compliance: Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (123156)	2	Trivial
Compliance: Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (123250)	2	Trivial
Compliance: Ensure 'Allow Remote Shell Access' is set to 'Disabled' (123253)	2	Trivial
Compliance: Ensure 'Allow search and Cortana to use location' is set to 'Disabled' (123228)	2	Trivial
Compliance: Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (123237)	2	Trivial
Compliance: Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]' (123181)	2	Trivial
Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (123251)	2	Trivial
Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (123247)	2	Trivial
Compliance: Ensure 'Allow Use of Camera' is set to 'Disabled' (123176)	2	Trivial
Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (123240)	2	Trivial
Compliance: Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On' (123238)	2	Trivial
Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (123241)	2	Trivial

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (123216)	2	Trivial
Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123185)	2	Trivial
Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (123186)	2	Trivial
Compliance: Ensure 'Audit Account Lockout' is set to 'Success and Failure' (123059)	2	Trivial
Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (123049)	2	Trivial
Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (123066)	2	Trivial
Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (123067)	2	Trivial
Compliance: Ensure 'Audit Authorization Policy Change' is set to 'Success' (123068)	2	Trivial
Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (123050)	2	Trivial
Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (123048)	2	Trivial
Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (122949)	2	Trivial
Compliance: Ensure 'Audit Group Membership' is set to 'Success' (123060)	2	Trivial
Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (123070)	2	Trivial
Compliance: Ensure 'Audit Logoff' is set to 'Success' (123061)	2	Trivial
Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (123062)	2	Trivial
Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (123052)	2	Trivial

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (123063)	2	Trivial
Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (123071)	2	Trivial
Compliance: Ensure 'Audit PNP Activity' is set to 'Success' (123055)	2	Trivial
Compliance: Ensure 'Audit Process Creation' is set to 'Success' (123056)	2	Trivial
Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (123065)	2	Trivial
Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (123053)	2	Trivial
Compliance: Ensure 'Audit Security State Change' is set to 'Success' (123072)	2	Trivial
Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (123073)	2	Trivial
Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (123069)	2	Trivial
Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (122950)	2	Trivial
Compliance: Ensure 'Audit Special Logon' is set to 'Success' (123064)	2	Trivial
Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (123074)	2	Trivial
Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (123054)	2	Trivial
Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (122905)	2	Trivial
Compliance: Ensure 'Block launching Windows Store apps with Windows Runtime API access from hosted content.' is set to 'Enabled' (123171)	2	Trivial
Compliance: Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (123148)	2	Trivial
Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (123126)	2	Trivial

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (122906)	2	Trivial
Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (122907)	2	Trivial
Compliance: Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (123115)	2	Trivial
Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (123259)	2	Trivial
Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (123260)	2	Trivial
Compliance: Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party cookies' or higher (123200)	2	Trivial
Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (123159)	2	Trivial
Compliance: Ensure 'Configure Password Manager' is set to 'Disabled' (123201)	2	Trivial
Compliance: Ensure 'Configure Pop-up Blocker' is set to 'Enabled' (123202)	2	Trivial
Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (123127)	2	Trivial
Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (123128)	2	Trivial
Compliance: Ensure 'Configure search suggestions in Address bar' is set to 'Disabled' (123203)	2	Trivial
Compliance: Ensure 'Configure SmartScreen Filter' is set to 'Enabled' (123204)	2	Trivial
Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (123160)	2	Trivial
Compliance: Ensure 'Configure Watson events' is set to 'Disabled' (123236)	2	Trivial
Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled' (123193)	2	Trivial

Compliance: Ensure 'Continue experiences on this device' is set to 'Disabled' (123129)	2	Trivial
Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (122908)	2	Trivial
Compliance: Ensure 'Create a token object' is set to 'No One' (122909)	2	Trivial
Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (122910)	2	Trivial
Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (122911)	2	Trivial
Compliance: Ensure 'Debug programs' is set to 'Administrators' (122914)	2	Trivial
Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (122917)	2	Trivial
Compliance: Ensure 'Deny log on as a service' to include 'Guests' (122918)	2	Trivial
Compliance: Ensure 'Deny log on locally' to include 'Guests' (122919)	2	Trivial
Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (122920)	2	Trivial
Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (122951)	2	Trivial
Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (122952)	2	Trivial
Compliance: Ensure 'Disable all apps from Windows Store' is set to 'Enabled' (123230)	2	Trivial
Compliance: Ensure 'Disable pre-release features or settings' is set to 'Disabled' (123182)	2	Trivial
Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (123172)	2	Trivial
Compliance: Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (123147)	2	Trivial
Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (123248)	2	Trivial

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (123252)	2	Trivial
Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (122956)	2	Trivial
Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (122957)	2	Trivial
Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (122958)	2	Trivial
Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (122959)	2	Trivial
Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (122960)	2	Trivial
Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (122962)	2	Trivial
Compliance: Ensure 'Do not allow COM port redirection' is set to 'Enabled' (123212)	2	Trivial
Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (123213)	2	Trivial
Compliance: Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (123214)	2	Trivial
Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (123210)	2	Trivial
Compliance: Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (123215)	2	Trivial
Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (123222)	2	Trivial
Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (123149)	2	Trivial
Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (123179)	2	Trivial
Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (123150)	2	Trivial

Compliance: Ensure 'Do not show feedback notifications' is set to 'Enabled' (123183)	2	Trivial
Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (123223)	2	Trivial
Compliance: Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (123164)	2	Trivial
Compliance: Ensure 'Enable Font Providers' is set to 'Disabled' (123098)	2	Trivial
Compliance: Ensure 'Enable insecure guest logons' is set to 'Disabled' (123099)	2	Trivial
Compliance: Ensure 'Enable Windows NTP Client' is set to 'Enabled' (123166)	2	Trivial
Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (122884)	2	Trivial
Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (123180)	2	Trivial
Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (123151)	2	Trivial
Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (122923)	2	Trivial
Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (122924)	2	Trivial
Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (123112)	2	Trivial
Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (123125)	2	Trivial
Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (122927)	2	Trivial
Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (122963)	2	Trivial
Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (122964)	2	Trivial

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (122965)	2	Trivial
Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (122970)	2	Trivial
Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (122973)	2	Trivial
Compliance: Ensure 'Join Microsoft MAPS' is set to 'Disabled' (123234)	2	Trivial
Compliance: Ensure 'Let Windows apps *' is set to 'Enabled: Force Deny' (123169)	2	Trivial
Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (122928)	2	Trivial
Compliance: Ensure 'Lock pages in memory' is set to 'No One' (122929)	2	Trivial
Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (122885)	2	Trivial
Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (122974)	2	Trivial
Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (122975)	2	Trivial
Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (122976)	2	Trivial
Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (122977)	2	Trivial
Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (122979)	2	Trivial
Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (122980)	2	Trivial
Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (122981)	2	Trivial
Compliance: Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (123163)	2	Trivial

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (123121)	2	Trivial
Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (122887)	2	Trivial
Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (122888)	2	Trivial
Compliance: Ensure 'Modify an object label' is set to 'No One' (122933)	2	Trivial
Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (122934)	2	Trivial
Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (123084)	2	Trivial
Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (123086)	2	Trivial
Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely ... (123085)	2	Trivial
Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (123087)	2	Trivial
Compliance: Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (123088)	2	Trivial
Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (123089)	2	Trivial
Compliance: Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (123090)	2	Trivial
Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (123091)	2	Trivial
Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (123092)	2	Trivial

Compliance: Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (123094)	2	Trivial
Compliance: Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (123093)	2	Trivial
Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (123095)	2	Trivial
Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (122983)	2	Trivial
Compliance: Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (122986)	2	Trivial
Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (122987)	2	Trivial
Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (122992)	2	Trivial
Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (122994)	2	Trivial
Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (122995)	2	Trivial
Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (122997)	2	Trivial
Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (122996)	2	Trivial
Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (122998)	2	Trivial
Compliance: Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (122999)	2	Trivial
Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (123000)	2	Trivial

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (123001)	2	Trivial
Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM&NTLM' (123002)	2	Trivial
Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (123003)	2	Trivial
Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (123004)	2	Trivial
Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (123005)	2	Trivial
Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (123261)	2	Trivial
Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (122889)	2	Trivial
Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (122935)	2	Trivial
Compliance: Ensure 'Prevent access to the about:flags page in Microsoft Edge' is set to 'Enabled' (123205)	2	Trivial
Compliance: Ensure 'Prevent bypassing SmartScreen prompts for files' is set to 'Enabled' (123206)	2	Trivial
Compliance: Ensure 'Prevent bypassing SmartScreen prompts for sites' is set to 'Enabled' (123207)	2	Trivial
Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (123224)	2	Trivial
Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (123075)	2	Trivial
Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (123076)	2	Trivial
Compliance: Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (123242)	2	Trivial

Compliance: Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (123209)	2	Trivial
Compliance: Ensure 'Prevent using Localhost IP address for WebRTC' is set to 'Enabled' (123208)	2	Trivial
Compliance: Ensure 'Profile single process' is set to 'Administrators' (122936)	2	Trivial
Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (122937)	2	Trivial
Compliance: Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (123120)	2	Trivial
Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (123109)	2	Trivial
Compliance: Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (123110)	2	Trivial
Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (122938)	2	Trivial
Compliance: Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (123157)	2	Trivial
Compliance: Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (123158)	2	Trivial
Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (123111)	2	Trivial
Compliance: Ensure 'Require pin for pairing' is set to 'Enabled' (123178)	2	Trivial
Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (123217)	2	Trivial
Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (122894)	2	Trivial
Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (122939)	2	Trivial
Compliance: Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (123211)	2	Trivial

Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123187)	2	Trivial
Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (123188)	2	Trivial
Compliance: Ensure 'Select when Feature Updates are received' is set to 'Enabled: Current Branch for Business, 180 days' (123254)	2	Trivial
Compliance: Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (123257)	2	Trivial
Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (123218)	2	Trivial
Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (123173)	2	Trivial
Compliance: Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less' (123219)	2	Trivial
Compliance: Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (123221)	2	Trivial
Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123189)	2	Trivial
Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (123190)	2	Trivial
Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (123006)	2	Trivial
Compliance: Ensure 'Shut down the system' is set to 'Administrators' (122940)	2	Trivial
Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (123243)	2	Trivial
Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (122890)	2	Trivial
Compliance: Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (123145)	2	Trivial
Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123191)	2	Trivial

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (123007)	2	Trivial
Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (123008)	2	Trivial
Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (123192)	2	Trivial
Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (122942)	2	Trivial
Compliance: Ensure 'Toggle user control over Insider builds' is set to 'Disabled' (123184)	2	Trivial
Compliance: Ensure 'Turn off access to the Store' is set to 'Enabled' (123131)	2	Trivial
Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (123152)	2	Trivial
Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (123231)	2	Trivial
Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (123174)	2	Trivial
Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (123130)	2	Trivial
Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (123194)	2	Trivial
Compliance: Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (123132)	2	Trivial
Compliance: Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (123133)	2	Trivial
Compliance: Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (123134)	2	Trivial
Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (123195)	2	Trivial
Compliance: Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (123135)	2	Trivial

Compliance: Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (123136)	2	Trivial
Compliance: Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (123229)	2	Trivial
Compliance: Ensure 'Turn off location' is set to 'Enabled' (123197)	2	Trivial
Compliance: Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (123177)	2	Trivial
Compliance: Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (123108)	2	Trivial
Compliance: Ensure 'Turn off printing over HTTP' is set to 'Enabled' (123137)	2	Trivial
Compliance: Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (123138)	2	Trivial
Compliance: Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (123139)	2	Trivial
Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (123196)	2	Trivial
Compliance: Ensure 'Turn off the advertising ID' is set to 'Enabled' (123165)	2	Trivial
Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (123232)	2	Trivial
Compliance: Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (123140)	2	Trivial
Compliance: Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (123141)	2	Trivial
Compliance: Ensure 'Turn off the Store application' is set to 'Enabled' (123233)	2	Trivial
Compliance: Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (123142)	2	Trivial
Compliance: Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (123143)	2	Trivial
Compliance: Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (123144)	2	Trivial

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (123153)	2	Trivial
Compliance: Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (123100)	2	Trivial
Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (123244)	2	Trivial
Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (123245)	2	Trivial
Compliance: Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (123104)	2	Trivial
Compliance: Ensure 'Untrusted Font Blocking' is set to 'Enabled: Block untrusted fonts and log events' (123154)	2	Trivial
Compliance: Ensure 'Use enhanced anti-spoofing when available' is set to 'Enabled' (123175)	2	Trivial
Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (123009)	2	Trivial
Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (123010)	2	Trivial
Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (123011)	2	Trivial
Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (123012)	2	Trivial
Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (123013)	2	Trivial
Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (123014)	2	Trivial
Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (123015)	2	Trivial
Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (123016)	2	Trivial

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (123017)	2	Trivial
Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (123124)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (123018)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (123019)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (123026)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (123027)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log' (123024)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (123025)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (123020)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (123023)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (123022)	2	Trivial
Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (123021)	2	Trivial
Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (123028)	2	Trivial
Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (123029)	2	Trivial
Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (123036)	2	Trivial
Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (123037)	2	Trivial

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log' (123034)	2	Trivial
Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (123035)	2	Trivial
Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (123030)	2	Trivial
Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (123033)	2	Trivial
Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (123032)	2	Trivial
Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (123031)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (123038)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (123039)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (123046)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (123047)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log' (123044)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (123045)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (123040)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (123043)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (123042)	2	Trivial
Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (123041)	2	Trivial

Echo Service (101032)	2	Trivial
Chargen Service (101021)	1	Trivial
Compliance: Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (122899)	1	Trivial
Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (123123)	1	Trivial
Compliance: Ensure 'Audit Directory Service Access' is set to 'Success and Failure' (DC only) (123057)	1	Trivial
Compliance: Ensure 'Audit Directory Service Changes' is set to 'Success and Failure' (DC only) (123058)	1	Trivial
Compliance: Ensure 'Audit Distribution Group Management' is set to 'Success and Failure' (DC only) (123051)	1	Trivial
Compliance: Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (122953)	1	Trivial
Compliance: Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (122954)	1	Trivial
Compliance: Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (122955)	1	Trivial
Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (123079)	1	Trivial
Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (123080)	1	Trivial
Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (123161)	1	Trivial
Compliance: Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (123167)	1	Trivial
Compliance: Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (122969)	1	Trivial
Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (122972)	1	Trivial

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (123078)	1	Trivial
Compliance: Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (122930)	1	Trivial
Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (122982)	1	Trivial
Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (122985)	1	Trivial
Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (122984)	1	Trivial
Compliance: Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (122993)	1	Trivial
Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (123083)	1	Trivial
Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (123081)	1	Trivial
Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (123082)	1	Trivial
Compliance: Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (123122)	1	Trivial
Compliance: Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (123162)	1	Trivial
Compliance: Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (122941)	1	Trivial
Compliance: Ensure 'Turn off multicast name resolution' is set to 'Enabled' (MS Only) (123097)	1	Trivial
Compliance: Set 'NetBIOS node type' to 'P-node' (Ensure NetBT Parameter 'NodeType' is set to '0x2 (2)') (MS Only) (123096)	1	Trivial
Daytime Service Detected (101026)	1	Trivial

Discard Service Detected (100370)	1	Trivial
ICMP Timestamp Request (150396)	1	Trivial
SMB Domain SID Disclosure (100872)	1	Trivial
Web Server Directory Structure Disclosure (104434)	1	Trivial

6 Assets Overview

A detailed summary of findings for each asset is presented in this section. These listings provide an in-depth view of the issues that were identified on a particular asset.

WIN-0NVC5M7BAU7	F

IP: 10.27.34.43
Asset name: WIN-0NVC5M7BAU7
Operating system: Windows Server 2008 R2 Enterprise
Asset type: Server

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	Failure

Vulnerability Title	Service(s)	Severity
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) internal | explicit | unauth	445 / tcp smb	Critical
This asset is missing the MS17-010 patch. Vulnerable Response: ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D.... 00 00 00 00 00 00 00 00 04 08 06 00 00 20 eb 3d ....= 00 00 00 ...		
Microsoft Windows Server 2008 R2 End of Life (131870) internal | explicit | unauth	N/A / tcp unknown	High

Support has ended for Windows Server 2008 R2. This host should be immediately upgraded.

MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756)

135 / tcp
msrpc

Medium

internal | **explicit** | **unauth**

```
This asset permits binding to samr pipe using auth level Connect.
Response from asset:
02 .

22 00 00 c0 "...

Responding port: 1030
```

SMB Security Signatures Not Required (104188)

445 / tcp
smb

Low

internal | **explicit** | **unauth**

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

SMB Null Session Authentication (101373)

445 / tcp
smb

Trivial

internal | **recon** | **unauth**

It was possible to log into the remote host using a NULL session.

SMB Native LanMan Version (100092)

445 / tcp
smb

Trivial

internal | **recon** | **unauth**

LAN Manager: Windows Server 2008 R2 Enterprise 6.1
Domain: WORKGROUP
OS: Windows Server 2008 R2 Enterprise 7601 Service Pack 1

ubuntu.internal.cloudapp.net

F

IP: 10.27.34.67
Asset name: ubuntu.internal.cloudapp.net
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
smb	139 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Samba IsKnownPipename Remote Code Execution (122062) internal | explicit | unauth	139 / tcp smb	Critical
This asset is missing the CVE-2017-7494 patch Payload: nirv32.so Share: cherlengue Physical path: /sambarepo/nirv32.so Successful Exploitation: Successfully retreived touch file		
PHP Multiple Type Confusion Denial of Service Vulnerabilities (273413) internal | potential | unauth	80 / tcp http	High
5.5.9		
Samba Remote Code Execution Vulnerability (126509) internal | potential | unauth	139 / tcp smb	High
4.3.11		
PHP 'tar.c' Stack Buffer Overflow (276915) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'incomplete_class.c' Type Confusion Denial of Service (273414) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP phar_object.c 'phar_convert_to_other' Denial of Service (275411) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'zend_exceptions.c' Type Confusion Remote Code Execution (273415) internal | potential | unauth	80 / tcp http	High
5.5.9		

PHP 'escapeshellarg' Function Remote Command Execution Vulnerability (278617) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
PHP 'soap.c' Type Confusion Denial of Service (273411) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
PHP SoapClient Multiple Type Confusion Denial of Service Vulnerabilities (273412) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
PHP php_http.c 'make_http_soap_request' Remote Code Execution (276912) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
Apache httpd '2.2.32 2.4.24' Remote Segmentation Fault Vulnerability (290291) **internal | potential | unauth**	80 / tcp http	High
2.4.7		
PHP sanitizing.c 'php_filter_encode' Integer Overflow Denial of Service (279636) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
Zend NULL Pointer Denial of Service (278089) **internal | potential | unauth**	80 / tcp http	High
php 5.5.9		
PHP WDDX Extension Use-after-free Vulnerability (276916) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
PHP xml.c 'xml_utf8_encode' Integer Overflow Denial of Service (279482) **internal | potential | unauth**	80 / tcp http	High

5.5.9		
Ruby 'Oniguruma-mod' and PHP unicode_unfold_key in 'mbstring' Buffer Overflow (289396) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'spl_ptr_heap_insert' Function Arbitrary Code Execution Vulnerability (278838) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'php_url_parse_ex' Denial of Service (277705) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP string.c 'str_pad' Denial of Service (280596) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP php_zip.c 'getFromIndex', 'getFromName' Heap Overflow (277149) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'locale_methods.c' Argument Overflow Denial of Service (283453) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'ext/phar/phar_object.c' Zero-length Uncompress Denial of Service (277155) internal | potential | unauth	80 / tcp http	High
5.5.9		
OpenSSH 'kbdint_next_device' Function Denial of Service (273895) internal | potential | unauth	22 / tcp ssh	High
6.6.1p1		

PHP CGI Component Command Execution Vulnerability (269957) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
OpenSSH 'ssh/kex.c' Denial of Service Vulnerability (126638) **internal | potential | unauth**	22 / tcp ssh	High
6.6.1p1		
OpenSSH 'ssh-agent.c' Untrusted Search Path Vulnerability (283439) **internal | potential | unauth**	22 / tcp ssh	High
6.6.1p1		
PHP wddx.c 'wddx_stack_destroy' Denial of Service Vulnerability (281194) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
PHP ext/standard/http_fopen_wrapper.c 'php_stream_url_wrap_http_ex' Stack-based Buffer Under-read (901430) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
PHP phar.c 'phar_parse_pharfile' Denial of Service (284034) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
PHP 'dynamicGetbuf' Denial of Service Vulnerability (127020) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
PHP 'process_nested_data' Function Use-After-Free Flaw (270531) **internal | potential | unauth**	80 / tcp http	High
5.5.9		
OpenSSH X11 Forwarding Access Bypass (276485) **internal | potential | unauth**	22 / tcp ssh	High
6.6.1p1		

PHP bcmath.c 'bcpowmod' Negative Integer Denial of Service (277157) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP before 5.5.36 and 5.6.x before 5.6.22 'php_html_entities' Function Denial of Service (280828) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP Session Deserializer 'php_var_unserialize' Remote Code Execution (275415) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'uncompressed_filesize' Crafted PHAR Archive Denial of Service Vulnerability (281199) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'ext/spl/spl_array.c' Use-after-free Remote Code Execution (275416) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP exif.c 'exif_process_IFD_TAG' Denial of Service (277162) internal | potential | unauth	80 / tcp http	High
5.5.9		
Ruby 'Oniguruma-mod' and PHP 'mbstring' Denial of Service (289391) internal | potential | unauth	80 / tcp http	High
5.5.9		
Apache HTTP Server Security Update 2.4.51 (147293) internal | potential | unauth	80 / tcp http	High
2.4.7		
Ruby 'Oniguruma-mod' and PHP 'mbstring' parse_char_class Denial of Service (289402) internal | potential | unauth	80 / tcp http	High

5.5.9

PHP 'simplestring_addn' Denial of Service Vulnerability (127019)

internal | potential | unauth

80 / tcp
http

High

5.5.9

Apache HTTP Server 'ap_get_basic_auth_pw' Authentication Bypass (290284)

internal | potential | unauth

80 / tcp
http

High

2.4.7

PHP 'phar_parse_metadata' Function Denial of Service (272818)

internal | potential | unauth

80 / tcp
http

High

5.5.9

Apache HTTP Server Security Update 2.4.48 (145498)

internal | potential | unauth

80 / tcp
http

High

2.4.7

PHP Zend Engine 'zend_ts_hash_graceful_destroy' Function Denial of Service Flaw (269858)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP 'pcntl_exec' Implementation File Extension Restriction Bypass (272809)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP Heap-Based Buffer Over-Read Vulnerability (127909)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP soap.c 'SoapClient__call' Arbitrary Code Execution (275418)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP spl_array.c 'SPL Extension' Denial of Service (280835)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP spl_array.c SplArray Unserialization Denial of Service (281201)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP 'phar_set_inode' Function Stack Buffer Overflow (272067)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP before 5.5.36 and 5.6.x before 5.6.22 'php_escape_html_entities_ex' Function Denial of Service (280829)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP 'gd_webp.c' Denial of Service Vulnerability (127034)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP wddx.c 'php_wddx_process_data' Denial of Service Vulnerability (281190)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP File Extension Restriction Bypass (272803)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP 'Serializable Interface, SplObjectStorage class, SplDoublyLinkedList class' Multiple Use-after-free Remote Code Execution (275414)

internal | potential | unauth

80 / tcp
http

High

5.5.9

Ruby 'Oniguruma-mod' and PHP fetch_token in 'mbstring' Denial of Service (289398)

internal | potential | unauth

80 / tcp
http

High

5.5.9

PHP Phar Extension 'phar_analyze_path' Arbitrary Code Execution (277153) **internal | potential | unauth**	80 / tcp http	High
	5.5.9	
PHP IMAP PHP Extension 'phar_fix_filepath' Function Buffer Overflow Vulnerability (275412) **internal | potential | unauth**	80 / tcp http	High
	5.5.9	
PHP var_unserializer.re Object Deserialization Denial of Service (281197) **internal | potential | unauth**	80 / tcp http	High
	5.5.9	
PHP 'wddx.c' XML Document Denial of Service (283454) **internal | potential | unauth**	80 / tcp http	High
	5.5.9	
PHP SPL 'ArrayObject, SplObjectStorage, SplDoublyLinkedList' Multiple Use-after-free Remote Code Execution (275413) **internal | potential | unauth**	80 / tcp http	High
	5.5.9	
PHP xml.c 'xml_parse_into_struct' Denial of Service (277159) **internal | potential | unauth**	80 / tcp http	High
	5.5.9	
PHP 'php_snmp_error' Function Format String Arbitrary Code Execution (277152) **internal | potential | unauth**	80 / tcp http	High
	5.5.9	
PHP zend_string_extend in 'Zend/zend_string.h' Denial of Service (288890) **internal | potential | unauth**	80 / tcp http	High
	5.5.9	
PHP 'ext/soap/soap.c' Type Confusion Vulnerability (272810) **internal | potential | unauth**	80 / tcp http	High

5.5.9		
PHP 'exif_process_IFD_in_TIFF' Uninitialized Read Vulnerability (128707) internal | potential | unauth	80 / tcp http	High
5.5.9		
Apache httpd '2.2.x before 2.2.33' and '2.4.x before 2.4.26' 'mod_ssl' subcomponent NULL pointer Vulnerability (290295) internal | potential | unauth	80 / tcp http	High
2.4.7		
PHP OPcache Extension '_zend_shared_memdup' Function Denial of Service Flaw (271046) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP Fileinfo Component 'apprentice_load' Denial of Service Flaw (269855) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'enchant_broker_request_dict' Function Arbitrary Code Execution (271564) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'ftp_genlist' Function LIST Command Buffer Overflow (273431) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP var_unserializer.c Invalid Object Denial of Service Vulnerability (281186) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP Fileinfo Component Crafted ELF File Denial of Service (271569) internal | potential | unauth	80 / tcp http	High
5.5.9		

Apache HTTP Server 2.4.53 Security Release (148390) internal | potential | unauth	80 / tcp http	High
2.4.7		
PHP exif.c 'exif_process_IFD_in_JPEG' Denial of Service (277163) internal | potential | unauth	80 / tcp http	High
5.5.9		
Fileinfo 'file_check_mem' Arbitrary Code Execution (277148) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP "phar_rename_archive" Function Denial of Service Flaw (271566) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'php_date.c' Multiple Use-After-Free Arbitrary Code Execution Flaws (271568) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP exif.c 'exif_process_TIFF_in_JPEG' Denial of Service (277164) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP wddx.c 'php_wddx_process_data' Double Free Vulnerability (280837) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP Wakeup Processing Denial of Service (283455) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP php_mbregex.c '_php_mb_regex_ereg_replace_exec' Double Free Vulnerability (280833) internal | potential | unauth	80 / tcp http	High
5.5.9		

PHP mbfilter.c 'mbfl_strcut' Integer Overflows Denial of Service (277154) internal | potential | unauth	80 / tcp http	High
5.5.9		
Ruby 'Oniguruma-mod' and PHP 'mbstring' forward_search_range Denial of Service (289394) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'curl_file.c' CURLFile Implementation Denial of Service (283441) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP spl_directory.c 'SplFileObject::fread' Denial of Service (282146) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'exif_process_IFD_in_MAKERNOTE' Denial of Service (277646) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP Invalid Memory Access Vulnerability (127908) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP mcrypt.c Multiple Integer Overflow Vulnerabilities (280834) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'var_unserializer.c' Integer Overflow (268708) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'snmp.c' Denial of Service (277774) internal | potential | unauth	80 / tcp http	High
5.5.9		

PHP gd.c 'imagegammacorrect' Input Validation Denial of Service Vulnerability (281188)
internal | potential | unauth
80 / tcp
http
High

5.5.9

PHP 'locale_accept_from_http' Denial of Service (277459)
internal | potential | unauth
80 / tcp
http
High

5.5.9

PHP SPL Component Type Confusion Vulnerability (265283)
internal | potential | unauth
80 / tcp
http
High

5.5.9

PHP php_zip.c Zip Extension Denial of Service (280836)
internal | potential | unauth
80 / tcp
http
High

5.5.9

PHP ZIP Extension "_zip_cdir_new" Function Integer Overflow (271576)
internal | potential | unauth
80 / tcp
http
High

5.5.9

PHP Multiple Heap-Based Buffer Over-Read Vulnerabilities (127911)
internal | potential | unauth
80 / tcp
http
High

5.5.9

Apache httpd '2.2.x before 2.2.33 and 2.4.x before 2.4.26' 'mod_mime' subcomponent Remote Read Vulnerability (290301)
internal | potential | unauth
80 / tcp
http
High

2.4.7

PHP grapheme.c 'grapheme_stripos' Denial of Service (277160)
internal | potential | unauth
80 / tcp
http
High

5.5.9

PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 'get_icu_value_internal' Function Denial of Service (280827)
internal | potential | unauth
80 / tcp
http
High

5.5.9

PHP gd.c 'imagetruecolortopalette' Input Validation Denial of Service Vulnerability (282235) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'var_unserializer.re' Use-after-free Vulnerability (269724) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP var_unserializer.re 'finish_nested_data' Buffer Overlow (292863) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP Pathname Sanitization Remote Arbitrary File Access Vulnerability (273410) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'session.c' Denial of Service (277689) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP spl_observer.c SplObjectStorage Unserialize Implementation Denial of Service (283532) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP grapheme_string.c 'graphme_strpos' Denial of Service (277161) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'process_nested_data' Function Use-After-Free Remote Code Execution Flaw (271575) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP 'ftp_genlist' Function Heap Buffer Overflow (272817) internal | potential | unauth	80 / tcp http	High

5.5.9		
PHP bcmath.c 'bcpowmod' Modified Data Structure Denial of Service (277158) internal | potential | unauth	80 / tcp http	High
5.5.9		
PHP before 5.5.36 and 5.6.x before 5.6.22 'file.c' Denial of Service (280830) internal | potential | unauth	80 / tcp http	High
5.5.9		
Samba '4.x before 4.7.3' Remote Code Execution Vulnerability (297439) internal | potential | unauth	139 / tcp smb	High
4.3.11		
OpenSSH 'session.c' Local Security Bypass Vulnerability (126635) internal | potential | unauth	22 / tcp ssh	High
6.6.1p1		
PHP 'sapi/fpm/fpm/fpm_unix.c' Privilege Escalation Vulnerability (126975) internal | potential | unauth	80 / tcp http	High
5.5.9		
OpenSSH Security Bypass Vulnerability (126647) internal | potential | unauth	22 / tcp ssh	High
6.6.1p1		
Apache HTTP Server 'mod_proxy_ftp' Uninitialized Memory Usage Vulnerability (133605) internal | potential | unauth	80 / tcp http	High
2.4.7		
OpenSSH 'ssh-agent' Double Free Vulnerability (144213) internal | potential | unauth	22 / tcp ssh	High
6.6.1p1		
Samba Security Advisory January 2022 (147947) internal | potential | unauth	139 / tcp smb	High

4.3.11		
libxml 'libxml_disable_entity_loader' XXE and XEE Vulnerability (278493) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 Remote Denial of Service Vulnerability (280831) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP phar.c 'phar_parse_pharfile' Denial of Service (290980) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
Samba November 2021 Security Update (146961) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		
PHP HTTP_PROXY Environment Variable Namespace Conflict (279443) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
OpenSSH 'scp' Command Evaluation Vulnerability (138013) **internal | potential | unauth**	22 / tcp ssh	Medium
6.6.1p1		
PHP php_variables.c Denial of Service (291000) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP "odbc_bindcols" Function Denial of Service Flaw (278354) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP 'Fileinfo' Component Denial of Service Vulnerability (127024) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		

OpenSSL Deprecated Function 'RAND_pseudo_bytes' (278298) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'mod_php' Or 'php-fpm' Information Disclosure (285650) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
NetBIOS Shares Accessible (100870) internal | explicit | unauth	139 / tcp smb	Medium
NetBIOS Shares: cherlengue		
Apache HTTP Server 'mod_http2' Module Denial of Service Vulnerability (282886) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
PHP 'var_unserializer.c' Denial of Service Vulnerability (126256) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP zend_exceptions.c Crafted Exception Object Denial of Service (283558) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
Apache HTTP Server Security Update 2.4.49 (146396) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Zend Recursive Method Denial of Service (278791) internal | potential | unauth	80 / tcp http	Medium
php 5.5.9		
PHP GMP Interfaces Denial of Service (287844) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP url.c 'parse_url' Restriction Bypass (290996) internal | potential | unauth	80 / tcp http	Medium

5.5.9

PHP 'linkinfo' File Path Disclosure Vulnerability (126959)
internal | potential | unauth
80 / tcp
http
Medium

5.5.9

PHP 'fsockopen' Server-Side Request Forgery Vulnerability (286727)
internal | potential | unauth
80 / tcp
http
Medium

5.5.9

PHP 'make_http_soap_request' Function Denial of Service (276913)
internal | potential | unauth
80 / tcp
http
Medium

5.5.9

OpenSSH Privilege Escalation Vulnerability (126645)
internal | potential | unauth
22 / tcp
ssh
Medium

6.6.1p1

OpenSSH monitor.c 'mm_answer_pam_free_ctx' Use-After-Free Vulnerability (126919)
internal | potential | unauth
22 / tcp
ssh
Medium

6.6.1p1

PHP Non-Blocking STDIN Stream Denial of Service Vulnerability (127023)
internal | potential | unauth
80 / tcp
http
Medium

5.5.9

Samba Symlink Denial of Service (289653)
internal | potential | unauth
139 / tcp
smb
Medium

4.3.11

Heimdal Man-in-the-Middle Vulnerability (291123)
internal | potential | unauth
139 / tcp
smb
Medium

4.3.11

Samba 'smbXcli_base.c' Man-In-The-Middle Client-Signing Protection Bypass (277364)
internal | potential | unauth
139 / tcp
smb
Medium

samba 4.3.11		
PHP 'php_handler' Function Denial of Service (272066) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
Apache HTTP Server 'mod_status' Module Race Condition (265518) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
PHP 'EXIF' Extension Crafted JPEG Denial of Service (268715) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP dns.c 'php_parserr' Function Buffer Overflow Denial of Service (266027) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP Zend Denial of Service Vulnerability (126972) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP '_gd2GetHeader' Denial of Service Vulnerability (127021) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP 'php_stream_zip_opener' Stack Buffer Overflow (277625) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP mysqlnd_wireprotocol.c BIT Field Heap Buffer Overflow (281198) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP bz2.c 'bzread' Denial of Service (280832) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		

PHP 'exif.c' Out-of-Bounds Read Vulnerability (126960) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP dirstream.c 'phar_make_dirstream' Mishandled Zero-size Denial of Service (277156) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'gdImageCreate' Denial of Service Vulnerability (127022) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP util.c 'phar_get_entry_data' Denial of Service (275603) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP zip.c 'phar_parse_zipfile' Denial of Service (275604) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'exif_process_unicode' Function EXIF Data Denial of Service Flaw (270518) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'virtual_file_ex' Stack Buffer Overflow (277731) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
Apache HTTP Server Multiple Vulnerabilities (126218) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
PHP 'gd_interpolation.c' Denial of Service Vulnerability (127028) internal | potential | unauth	80 / tcp http	Medium
5.5.9		

Samba 'ndr_pull_dnsp_name' Remote Privilege Escalation Vulnerability (126870) internal | potential | unauth	139 / tcp smb	Medium
4.3.11		
Samba Password Change Vulnerability (126513) internal | potential | unauth	139 / tcp smb	Medium
4.3.11		
Samba Input Validation Vulnerability (126518) internal | potential | unauth	139 / tcp smb	Medium
4.3.11		
Samba 'DelegationNotAllowed' Vulnerability (131863) internal | potential | unauth	139 / tcp smb	Medium
4.3.11		
Apache httpd Digest Authorization Denial of Service (291127) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
PHP Multiple Pathname Sanitization Remote Arbitrary File Access Vulnerabilities (273408) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 5.6.x and 7.x 'gdImageRotateInterpolated' Function Denial of Service (275989) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP gd_ctx.c Arbitrary File Overwrite Vulnerabilty (266023) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'sapi_header_op' Function Cross-Site Scripting Vulnerability (280826) internal | potential | unauth	80 / tcp http	Medium
5.5.9		

Samba Incorrect 'KDC' Implementation Vulnerability (129055) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		
Apache HTTP Server 'mod_auth_digest' Access Control Bypass Vulnerability (128444) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
PHP "main/php_open_temporary_file.c" Thread Safety Denial of Service Flaw (278227) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP mysqlnd Man in the Middle via Cleartext-downgrade (276914) **internal | potential | unauth**	80 / tcp http	Medium
php 5.5.9		
PHP 'ext/phar/phar.c' Buffer Over-read Vulnerability (272068) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
Samba Man in the Middle Hijack Vulnerability (126512) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		
OpenSSH scp Server Man-in-The-Middle Attack Vulnerability (127851) **internal | potential | unauth**	22 / tcp ssh	Medium
6.6.1p1		
Samba Man in the Middle Vulnerability (126511) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		
Apache HTTP Server 'mod_rewrite' Redirect Vulnerability (133604) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		

Apache HTTP Server URL Redirect Vulnerability (129591)
internal | potential | unauth
80 / tcp
http
Medium

2.4.7

OpenSSH Remote Command Injection Vulnerability (126646)
internal | potential | unauth
22 / tcp
ssh
Medium

6.6.1p1

Samba Registry Hive File Creation Vulnerability (128710)
internal | potential | unauth
139 / tcp
smb
Medium

4.3.11

OpenSSH 'auth-gss2.c' User Detection Vulnerability (126832)
internal | potential | unauth
22 / tcp
ssh
Medium

6.6.1p1

OpenSSH Sensitive Data Exposure Vulnerability (146710)
internal | potential | unauth
22 / tcp
ssh
Medium

6.6.1p1

OpenSSH 'ssh_packet_read_poll2' Function Denial of Service (275984)
internal | potential | unauth
22 / tcp
ssh
Medium

6.6.1p1

Apache HTTP Server HTTP_PROXY Environment Variable Vulnerability (126237)
internal | potential | unauth
80 / tcp
http
Medium

2.4.7

PHP xsltprocessor.c 'xsl_ext_function_php' Denial of Service During Initial Error Checking (275419)
internal | potential | unauth
80 / tcp
http
Medium

5.5.9

PHP 'ext/iconv/iconv.c' Infinite Loop Vulnerability (126961)
internal | potential | unauth
80 / tcp
http
Medium

5.5.9

Apache HTTP Server Padding Oracle Vulnerability (288579)

internal | potential | unauth

80 / tcp
http

Medium

2.4.7

PHP wddx.c 'wddx_deserialize' NULL Pointer Dereference Denial of Service Vulnerability (281193)

internal | potential | unauth

80 / tcp
http

Medium

5.5.9

PHP PostgreSQL Extension 'php_pgsql_meta_data' Function Denial of Service (273432)

internal | potential | unauth

80 / tcp
http

Medium

5.5.9

PHP 'value_len' Uninitialized Read Vulnerability (128704)

internal | potential | unauth

80 / tcp
http

Medium

5.5.9

PHP 'imagefilltoborder' Denial of Service (277172)

internal | potential | unauth

80 / tcp
http

Medium

5.5.9

PHP 'php_imap.c' Denial of Service Vulnerability (126280)

internal | potential | unauth

80 / tcp
http

Medium

5.5.9

Samba 'before 4.7.3' Possible Remote Sensitive Information Access Vulnerability (297423)

internal | potential | unauth

139 / tcp
smb

Medium

4.3.11

PHP 'mconvert' Function Denial of Service (265276)

internal | potential | unauth

80 / tcp
http

Medium

5.5.9

PHP phar.c 'phar_parse_pharfile' Denial of Service (284031)

internal | potential | unauth

80 / tcp
http

Medium

5.5.9

Apache HTTP Server 'lua_websocket_read' Function Denial of Service Vulnerability (126231) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
PHP exif.c 'exif_convert_any_to_int' Denial of Service (284033) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'exif.c' Integer Overflow Vulnerability (126957) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'phar_parse_tarfile' Function Denial of Service (272802) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'cdf_read_property_info' in Fileinfo Component Denial of Service (264496) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
Apache HTTP Server 'mod_session_cookie' Expiry Time Ignored Vulnerability (126276) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
PHP 'cdf_unpack_summary_info' in Fileinfo Component Denial of Service (264495) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'data_len' Uninitialized Read Vulnerability (128705) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
Apache 'Optionsbleed' UAF Memory Leak (122625) internal | potential | unauth	80 / tcp http	Medium
2.4.7		

PHP 'move_uploaded_file' Extension Restrictions Bypass Flaw (271565) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'gd_crop.c' Denial of Service Vulnerability (126980) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP exif.c 'exif_process_IFD_in_TIFF' Information Disclosure (281189) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'stream_resolve_include_path ' Function Pathname Sanitization Remote Arbitrary File Access Vulnerability (273409) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP PharData 'extractTo' Directory Traversal (275417) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP XMLRPC Extension Denial of Service (268706) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP wddx.c XML Deserialization Denial of Service (290987) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP msgformat_format.c 'MessageFormatter::formatMessage' Denial of Service Vulnerability (281200) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP gd_interpolation.c 'gdImageScaleTwoPass' Denial of Service (277173) internal | potential | unauth	80 / tcp http	Medium
5.5.9		

PHP parse_date.c 'php_parse_date' Information Disclosure (290999)

80 / tcp

http

Medium

internal | potential | unauth

5.5.9

PHP wddx.c 'php_wddx_pop_element' NULL Pointer Dereference Denial of Service Vulnerability (281191)

80 / tcp

http

Medium

internal | potential | unauth

5.5.9

Apache HTTP Server Digest Authentication Denial of Service (288580)

80 / tcp

http

Medium

internal | potential | unauth

2.4.7

PHP PostgreSQL 'build_tablename' Function Denial of Service Flaw (271047)

80 / tcp

http

Medium

internal | potential | unauth

5.5.9

PHP 'exif_process_SOFn' Invalid Read Vulnerability (128706)

80 / tcp

http

Medium

internal | potential | unauth

5.5.9

Apache HTTP Server HTTP Chunked Request Smuggling Attack (126232)

80 / tcp

http

Medium

internal | potential | unauth

2.4.7

PHP 'multipart_buffer_headers' Function Algorithmic Complexity Vulnerability (272827)

80 / tcp

http

Medium

internal | potential | unauth

5.5.9

PHP 'mget' Function Fileinfo Component Denial of Service (273416)

80 / tcp

http

Medium

internal | potential | unauth

5.5.9

OpenSSH 'before 7.6' 'process_open function in sftp-server.c' subcomponent Does not Properly Prevent Write Operations in Readonly Mode Vulnerability (296108) **internal | potential | unauth**	22 / tcp ssh	Medium
6.6.1p1		
Apache HTTP Server Response Splitting Vulnerability (288581) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server ' mod_log_config' Denial of Service (263002) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_dav' Denial of Service (263007) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_cache_socache' Out of Bound Read Denial of Service Vulnerability (126242) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
PHP wddx.c 'wddx_deserialize' NULL Pointer Dereference Denial of Service Vulnerability (281192) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP var_unserializer.c 'object_common1' Denial of Service (284032) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP 'ext/ldap/ldap.c' Denial of Service Vulnerability (126962) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP wddx.c 'php_wddx_push_element' Denial of Service (281202) **internal | potential | unauth**	80 / tcp http	Medium

5.5.9		
PHP openssl.c Denial of Service (290992) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
Apache HTTP Server 'cache_merge_headers_out' Function Denial of Service Vulnerability (126230) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
PHP 'mcopy' Function Fileinfo Component Denial of Service (273417) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'do_soap_call' Function Type Confusion Vulnerability (272828) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP Fileinfo Component Pascal String Denial of Service Flaw (271045) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'xmlrpc_decode()' Memory Over-Read Vulnerability (127912) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'php_raw_url_encode' Denial of Service (277151) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP xsltprocessor.c 'xsl_ext_function_php' Denial of Service During Principal Argument Loop (275420) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP session.c Invalid Session Names Object Injection (281187) internal | potential | unauth	80 / tcp http	Medium

	5.5.9		
PHP 'GetCode_' Function Crafted GIF Image Denial of Service (271572) internal | potential | unauth		80 / tcp http	Medium
	5.5.9		
Ruby 'Oniguruma-mod' and PHP 'mbstring' forward_search_range Denial of Service (289404) internal | potential | unauth		80 / tcp http	Medium
	5.5.9		
PHP 'before 5.6.32, 7.x before 7.0.25, 7.1.x before 7.1.11' Interpreter Information Leak Vulnerability (296552) internal | potential | unauth		80 / tcp http	Medium
	5.5.9		
OpenSSH User Enumeration Vulnerability (126863) internal | potential | unauth		22 / tcp ssh	Medium
	6.6.1p1		
OpenSSH kex.c and packet.c NULL Pointer Dereference Denial of Service (299655) internal | potential | unauth		22 / tcp ssh	Medium
	6.6.1p1		
Apache HTTP Server 'httpd' URL Normalization Inconsistency Vulnerability (128448) internal | potential | unauth		80 / tcp http	Medium
	2.4.7		
Apache HTTP "RequestHeader unset" Directive Bypass Vulnerability (126217) internal | potential | unauth		80 / tcp http	Medium
	2.4.7		
PHP 'gd.c' Denial of Service Vulnerability (126992) internal | potential | unauth		80 / tcp http	Medium
	5.5.9		

PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3: Metadata can be set by an attacker (900437)

internal | potential | unauth

80 / tcp

http

Medium

5.5.9

Apache HTTP Server winnt_accept Function Denial of Service (265505)

internal | potential | unauth

80 / tcp

http

Medium

2.4.7

Apache HTTP Server 'mod_cgid' Module Denial of Service (265538)

internal | potential | unauth

80 / tcp

http

Medium

2.4.7

PHP 'wddx.c' PDORow String Denial of Service (283445)

internal | potential | unauth

80 / tcp

http

Medium

5.5.9

PHP 'rename()' Sensitive Data Disclosure Vulnerability (128703)

internal | potential | unauth

80 / tcp

http

Medium

5.5.9

Samba Server Memory Information Leak over SMB1 (126510)

internal | potential | unauth

139 / tcp

smb

Medium

4.3.11

PHP WSDL Injection Attack Vulnerability (127026)

internal | potential | unauth

80 / tcp

http

Medium

5.5.9

OpenSSH Heap-Based Buffer Overflow Vulnerability (126642)

internal | potential | unauth

22 / tcp

ssh

Medium

6.6.1p1

PHP 'ext/spl/spl_dllist.c' Denial of Service Vulnerability (127031)

internal | potential | unauth

80 / tcp

http

Medium

5.5.9

PHP 'ext/spl/spl_array.c' Denial of Service Vulnerability (127032) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
OpenSSH Privilege Escalation Vulnerability (146711) internal | potential | unauth	22 / tcp ssh	Medium
6.6.1p1		
Samba Unauthorized File Creation Vulnerability (131710) internal | potential | unauth	139 / tcp smb	Medium
4.3.11		
Apache HTTP Server 'mod_lua' Access Restriction Bypass Vulnerability (269848) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
PHP cdf.c Integer Overflow Denial of Service (266029) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP JPEG Denial of Service Vulnerability (126958) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'exif_process_user_comment' Denial of Service (277618) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
Apache HTTP Server 'mod_userdir' CRLF Injection Vulnerability (126838) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
PHP 'Bucket Brigade' Vulnerability (126955) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP gd_gif_in.c Crafted GIF Denial of Service (299341) internal | potential | unauth	80 / tcp http	Medium

5.5.9		
Apache HTTP Server 'deflate_in_filter' Function Denial of Service (265521) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
PHP 'cdf_count_chain' Function Denial of Service (265272) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP 'ZipArchive::extractTo' Function Directory Traversal (276911) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
Apache HTTP Server 'mod_proxy' Cross-Site Scripting Vulnerability (129590) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_proxy' Module Denial of Service (265530) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
PHP gd_gif_in.c 'gdImageCreateFromGifCtx' Information Disclosure (291957) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP 'cdf_read_property_info' Function Denial of Service (265277) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		
PHP PHAR 404 Error Page Reflected Cross-Site Scripting (299348) **internal | potential | unauth**	80 / tcp http	Medium
5.5.9		

PHP Fileinfo Component Denial of Service (265273) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'cdf_check_stream_offset' Function Denial of Service (265280) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
PHP 'ext/phar/phar_object.c' Cross-site Scripting Vulnerability (126963) internal | potential | unauth	80 / tcp http	Medium
5.5.9		
Apache HTTP Server 'ap_some_auth_required' Function Remote Access Restrictions Bypass Vulnerability (273795) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
OpenSSH Account Enumeration Vulnerability (126640) internal | potential | unauth	22 / tcp ssh	Medium
6.6.1p1		
OpenSSH 'x11_open_helper' Function Access Restriction Bypass (273896) internal | potential | unauth	22 / tcp ssh	Medium
6.6.1p1		
OpenSSH 'Observable Discrepancy' Man-in-the-Middle Vulnerability (137503) internal | potential | unauth	22 / tcp ssh	Medium
6.6.1p1		
OpenSSH BLOWFISH Hashing User Enumeration (280859) internal | potential | unauth	22 / tcp ssh	Medium
6.6.1p1		
Samba 'LDAP' Server Denial of Service Vulnerability (126834) internal | potential | unauth	139 / tcp smb	Medium
4.3.11		

OpenSSH Information Disclosure Vulnerability (126643) **internal | potential | unauth**	22 / tcp ssh	Medium
6.6.1p1		
Samba 'LDAP' Search Denial of Service Vulnerability (126956) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		
Samba 'PAC' Checksum Denial of Service Vulnerability (126872) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		
Samba 'KDC' Denial of Service Vulnerability (127055) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		
Samba Confidential Attribute Values Disclosure Vulnerability (126516) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		
OpenSSH 'stderr' Man-in-The-Middle Attack Vulnerability (127850) **internal | potential | unauth**	22 / tcp ssh	Medium
6.6.1p1		
OpenSSH Missing Character Man-in-The-Middle Attack Vulnerability (127849) **internal | potential | unauth**	22 / tcp ssh	Medium
6.6.1p1		
Samba 'dirsync' Denial of Service Vulnerability (131712) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		
Samba 'DNS' Denial of Service Vulnerability (131862) **internal | potential | unauth**	139 / tcp smb	Medium
4.3.11		

Samba Kerberos Impersonation Vulnerability (126871) **internal | potential | unauth**	139 / tcp smb	Medium
	4.3.11	
Insecure Crossdomain.xml Directives (104181) **internal | explicit | unauth**	80 / tcp http	Low
	Path: /crossdomain.xml Content: <?xml version="1.0"?><cross-domain-policy><allow-access-from domain="*" /></cross-domain-policy>	
PHP 'gdImageColorMatch' Buffer Overflow Vulnerability (127853) **internal | potential | unauth**	80 / tcp http	Low
	5.5.9	
NetBIOS Shares With Everyone/Full-Control Permissions (104589) **internal | explicit | unauth**	139 / tcp smb	Low
	NetBIOS Everyone Accessible Shares: cherlengue (READ/WRITE)	
Apache HTTP Server mod_cluster Improper Input Validation Vulnerability (126238) **internal | potential | unauth**	80 / tcp http	Low
	2.4.7	
OpenSSH Security Advisory (148395) **internal | potential | unauth**	22 / tcp ssh	Low
	6.6.1p1	
PHP PEAR_REST Arbitrary File Write Vulnerability (127016) **internal | potential | unauth**	80 / tcp http	Low
	5.5.9	
PHP '/tmp/phpglibccheck' File Overwrite Vulnerability (127030) **internal | potential | unauth**	80 / tcp http	Low
	5.5.9	
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp smb	Low
	SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required	

OpenSSH scp Client Access Bypass Vulnerability (127848) | 22 / tcp | Low
internal | potential | unauth | ssh

6.6.1p1

PHP 'ext/standard/info.c' Sensitive Information Disclosure (127033) | 80 / tcp | Low
internal | potential | unauth | http

5.5.9

OpenSSH Local Information Disclosure Vulnerability (126644) | 22 / tcp | Low
internal | potential | unauth | ssh

6.6.1p1

OpenSSH 'sshd' Monitor Component Local Impersonation Vulnerability (274384) | 22 / tcp | Low
internal | potential | unauth | ssh

6.6.1p1

PHP 'PHP-FPM' Information Disclosure Vulnerability (126964) | 80 / tcp | Low
internal | potential | unauth | http

5.5.9

PHP End of Life (112906) | 80 / tcp | Low
internal | explicit | unauth | http

Version 5.5.9 of PHP has reached end-of-life status.

SMB Null Session Authentication (101373) | 139 / tcp | Trivial
internal | recon | unauth | smb

It was possible to log into the remote host using a NULL session.

Content Security Policy Missing (148043) | 80 / tcp | Trivial
internal | explicit | unauth | http

Missing Content Security Policy.

SMB Native LanMan Version (100092) | 139 / tcp | Trivial
internal | recon | unauth | smb

LAN Manager: Samba 4.3.11
Domain: WORKGROUP
OS: Windows 6.1

test-virtual-machine.internal.cloudapp.net **F**

IP: 10.27.34.83
Asset name: test-virtual-machine.internal.cloudapp.net
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) internal | explicit | unauth	22 / tcp ssh	Critical
successfully logged in with username: test, password: test		
OpenSSH 'ssh-agent.c' Untrusted Search Path Vulnerability (283439) internal | potential | unauth	22 / tcp ssh	High
7.2p2		
OpenSSH 'ssh/kex.c' Denial of Service Vulnerability (126638) internal | potential | unauth	22 / tcp ssh	High
7.2p2		
OpenSSH 'session.c' Local Security Bypass Vulnerability (126635) internal | potential | unauth	22 / tcp ssh	High
7.2p2		
OpenSSH Security Bypass Vulnerability (126647) internal | potential | unauth	22 / tcp ssh	High
7.2p2		
OpenSSH 'ssh-agent' Double Free Vulnerability (144213) internal | potential | unauth	22 / tcp ssh	High

7.2p2		
OpenSSH 'scp' Command Evaluation Vulnerability (138013) internal | potential | unauth	22 / tcp ssh	Medium
7.2p2		
OpenSSH Privilege Escalation Vulnerability (126645) internal | potential | unauth	22 / tcp ssh	Medium
7.2p2		
OpenSSH scp Server Man-in-The-Middle Attack Vulnerability (127851) internal | potential | unauth	22 / tcp ssh	Medium
7.2p2		
OpenSSH Sensitive Data Exposure Vulnerability (146710) internal | potential | unauth	22 / tcp ssh	Medium
7.2p2		
OpenSSH 'auth-gss2.c' User Detection Vulnerability (126832) internal | potential | unauth	22 / tcp ssh	Medium
7.2p2		
OpenSSH kex.c and packet.c NULL Pointer Dereference Denial of Service (299655) internal | potential | unauth	22 / tcp ssh	Medium
openssh 7.2 p2		
OpenSSH 'before 7.6' 'process_open function in sftp-server.c' subcomponent Does not Properly Prevent Write Operations in Readonly Mode Vulnerability (296108) internal | potential | unauth	22 / tcp ssh	Medium
openssh 7.2 p2		
OpenSSH User Enumeration Vulnerability (126863) internal | potential | unauth	22 / tcp ssh	Medium
7.2p2		
OpenSSH Privilege Escalation Vulnerability (146711) internal | potential | unauth	22 / tcp ssh	Medium

7.2p2		
OpenSSH Account Enumeration Vulnerability (126640) **internal | potential | unauth**	22 / tcp ssh	Medium
7.2p2		
OpenSSH 'Observable Discrepancy' Man-in-the-Middle Vulnerability (137503) **internal | potential | unauth**	22 / tcp ssh	Medium
7.2p2		
OpenSSH BLOWFISH Hashing User Enumeration (280859) **internal | potential | unauth**	22 / tcp ssh	Medium
openssh 7.2 p2		
OpenSSH 'stderr' Man-in-The-Middle Attack Vulnerability (127850) **internal | potential | unauth**	22 / tcp ssh	Medium
7.2p2		
OpenSSH Missing Character Man-in-The-Middle Attack Vulnerability (127849) **internal | potential | unauth**	22 / tcp ssh	Medium
7.2p2		
OpenSSH Security Advisory (148395) **internal | potential | unauth**	22 / tcp ssh	Low
7.2p2		
OpenSSH scp Client Access Bypass Vulnerability (127848) **internal | potential | unauth**	22 / tcp ssh	Low
7.2p2		
OpenSSH Local Information Disclosure Vulnerability (126644) **internal | potential | unauth**	22 / tcp ssh	Low
7.2p2		

demo.testfire.net **F**

IP: 65.61.137.117
Asset name: demo.testfire.net
Operating system: unknown

Asset type: Server

Protocol	Service
http	80 / tcp
http	8080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
HTTP Easily Guessable Credentials (104433) **external** | **explicit** | **unauth**	8080 / tcp http	Critical
Authentication Successful In Forms: demo.testfire.net:8080: /login.jsp : login: admin:admin		
Slowloris Resource Depletion And Denial Of Service (104012) **external** | **explicit** | **unauth**	8080 / tcp http	Medium
The webserver appears to be vulnerable to a resource exhaustion attack.		
Web Server Uses Unencrypted/Plaintext Form Password Fields (103980) **external** | **explicit** | **unauth**	8080 / tcp http	Low
Password forms post to non-ssl: demo.testfire.net:8080: /login.jsp : login		
Web Server Directory Structure Disclosure (104434) **external** | **recon** | **unauth**	8080 / tcp http	Trivial
Internal File Structure Disclosed: demo.testfire.net:8080: Error response from /feedback.jsp: L:\backup\website\oldfiles ---		

192.168.67.3	F

IP: 192.168.67.3

Asset name: 192.168.67.3
Operating system: Debian 9 Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
successfully logged in with username: user, password: user		
Phpinfo.php System Information Disclosure (100403) **internal** | **explicit** | **unauth**	80 / tcp http	Low
[Large data section omitted]		
HTTP Host Header Value Reflection (128596) **internal** | **explicit** | **unauth**	80 / tcp http	Low
/manual : an't connect to vm.frontline.cloud:80 (Bad hostnam		
Apache Manual Page Information Leak (103390) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Apache 2.4 documentation page detected.		
Debian End of Life (134009) **internal** | **explicit** | **unauth**	22 / tcp ssh	Low
Debian 9.0 has reached end-of-life status.		
Content Security Policy Missing (148043) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial

	Missing Content Security Policy.		
Web Server Default Error Page Detected (128223) internal | explicit | unauth		80 / tcp http	Trivial
	[Large data section omitted]		

Asset Comments and Notes

Comment | Sohail Moiz (sohail.moiz@helpsystems.com) | Tuesday, Oct. 25, 2022 1:10 PM CDT
example 2

Comment | Sohail Moiz (sohail.moiz@helpsystems.com) | Tuesday, Oct. 25, 2022 1:09 PM CDT
example

192.168.67.52 F

IP: 192.168.67.52
Asset name: 192.168.67.52
Operating system: Debian 9 Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) internal | explicit | unauth	22 / tcp ssh	Critical
successfully logged in with username: user, password: user		
Debian End of Life (134009) internal | explicit | unauth	22 / tcp ssh	Low
Debian 9.0 has reached end-of-life status.		

Asset Comments and Notes
Comment | Sohail Moiz (sohail.moiz@helpsystems.com) | Tuesday, Oct. 25, 2022 1:09 PM CDT example
Hidden Note | Sohail Moiz (sohail.moiz@helpsystems.com) | Monday, July 18, 2022 10:48 AM CDT Test

192.168.67.52 F

IP: 192.168.67.52
Asset name: 192.168.67.52
Operating system: Debian 9 Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
successfully logged in with username: user, password: user		
Debian End of Life (134009) **internal** | **explicit** | **unauth**	22 / tcp ssh	Low
Debian 9.0 has reached end-of-life status.		

COMPUTER F

IP: 192.168.67.53
Asset name: COMPUTER
Operating system: Windows Server 2008
Asset type: Server

Protocol	Service

msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
MS09-050 Microsoft Windows SMB2 Command Execution Vulnerabilities (Network Check) (104045) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
MS09-050		
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
This asset is missing the MS17-010 patch. Vulnerable Response: ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D.... 00 00 00 00 00 00 00 00 05 b0 06 00 02 88 46 f2 ....F. 00 00 00 ...		
Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST 11/18 - Patch Applied		
Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT remediated on 5/24		
Microsoft Windows Server 2008 End of Life (131869) **internal** | **explicit** | **unauth**	N/A / tcp unknown	High
Support has ended for Windows Server 2008. This host should be immediately upgraded.		
MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133) **internal** | **explicit** | **unauth**	445 / tcp smb	Medium
MS10-012 Weak NTLM Session Key Detected: (1085552fd5fb5b11)		

MS11-020: SMB Transaction Parsing Vulnerability (Network Check) (104422) internal | explicit | unauth	445 / tcp smb	Medium
ms11-020		
SMB Security Signatures Not Required (104188) internal | explicit | unauth	445 / tcp smb	Low
SMBv1 NTLM signatures are not required		
Microsoft Windows Service Pack Outdated (104065) internal | explicit | unauth	445 / tcp smb	Low
Windows 2008 Service Pack 2 is not installed		
SMB Null Session Authentication (101373) internal | recon | unauth	445 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		
SMB Native LanMan Version (100092) internal | recon | unauth	445 / tcp smb	Trivial
LAN Manager: Windows Server (R) 2008 Standard without Hyper-V 6.0 Domain: WORKGROUP OS: Windows Server (R) 2008 Standard without Hyper-V 6001 Service Pack 1		

192.168.67.54 F

IP: 192.168.67.54
Asset name: 192.168.67.54
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: admin, password: admin		
Content Security Policy Missing (148043) **internal | explicit | unauth**	80 / tcp http	Trivial
Missing Content Security Policy.		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		

BUFF-HEARTBLEED

F

IP: 192.168.67.55
Asset name: BUFF-HEARTBLEED
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
http	80 / tcp
pop3	110 / tcp
netbios-ns	137 / udp
smb	139 / tcp
imap	143 / tcp
http (ssl)	443 / tcp
imap (ssl)	993 / tcp
pop3 (ssl)	995 / tcp

jdwp	8000 / tcp
http	8080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	993 / tcp imap (ssl)	Critical
[Large data section omitted]		
Comment | Robert Mercier (788 robert.mercier@digitaldefense.com) | Saturday, March 9, 2019 9:16 PM CST Will fix 1-3-19		
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	110 / tcp pop3	Critical
[Large data section omitted]		
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	995 / tcp pop3 (ssl)	Critical
[Large data section omitted]		
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	143 / tcp imap	Critical
[Large data section omitted]		
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Critical
[Large data section omitted]		
NetBIOS Shares Accessible (100870) **internal** | **explicit** | **unauth**	139 / tcp smb	Medium
NetBIOS Accessible Shares: myshare (READ/WRITE)		

Java Debugging Port Accessible (104527)

8000 / tcp
jdwp

Medium

internal | **explicit** | **unauth**

```
Java Debug Wire Protocol (Reference Implementation) version 1.6
JVM Debug Interface version 1.2
JVM version 1.6.0_27 (OpenJDK Client VM, mixed mode, sharing)1.6.0_27OpenJDK Client VM
```

SMB Writeable Directories (104477)

139 / tcp
smb

Medium

internal | **explicit** | **unauth**

```
Writeable Directories
Share name 'myshare':
\
```

Web Server Directory Indexing Enabled (101049)

80 / tcp
http

Low

internal | **explicit** | **unauth**

```
Directory Indexing Enabled:
192.168.67.55:80:

/keys
```

SSL Connection: Server Appears Vulnerable to ChangeCipherSpec Injection (115134)

443 / tcp
http (ssl)

Low

internal | **explicit** | **unauth**

```
Host does not reject early change cipher spec using TLSv1.1
Host does not reject early change cipher spec using TLSv1
Host does not reject early change cipher spec using SSLv3
```

SSL Connection: Server Appears Vulnerable to ChangeCipherSpec Injection (115134)

993 / tcp
imap (ssl)

Low

internal | **explicit** | **unauth**

```
Host does not reject early change cipher spec using TLSv1.2
Host does not reject early change cipher spec using TLSv1.1
Host does not reject early change cipher spec using TLSv1
Host does not reject early change cipher spec using SSLv3
```

Slowloris Resource Depletion And Denial Of Service (117854)

8080 / tcp
http

Low

internal | **explicit** | **unauth**

```
The webserver appears to be vulnerable to a resource exhaustion attack.
```

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

110 / tcp
pop3

Low

internal | **explicit** | **unauth**

```
[Large data section omitted]
```

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

993 / tcp
imap (ssl)

Low

internal | **explicit** | **unauth**

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) internal | explicit | unauth	995 / tcp pop3 (ssl)	Low

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) internal | explicit | unauth	143 / tcp imap	Low

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) internal | explicit | unauth	443 / tcp http (ssl)	Low

[Large data section omitted]

SSL Connection: RSA Export Grade Cipher FREAK Vulnerability (117845) internal | explicit | unauth	443 / tcp http (ssl)	Low

[Large data section omitted]

SSL Connection: TLS Diffie-Hellman Export Cipher Downgrade Logjam Vulnerability (117846) internal | explicit | unauth	443 / tcp http (ssl)	Low

```
EXP-EDH-RSA-DES-CBC-SHA - TLSv1
EXP-EDH-RSA-DES-CBC-SHA - TLSv11
EXP-EDH-RSA-DES-CBC-SHA - TLSv12
```

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843) internal | explicit | unauth	443 / tcp http (ssl)	Low

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843) internal | explicit | unauth	993 / tcp imap (ssl)	Low

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843) internal | explicit | unauth	995 / tcp pop3 (ssl)	Low

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SMB Security Signatures Not Required (104188) 139 / tcp Low
internal | explicit | unauth smb

SMBv1 NTLM signatures are not required

ISC BIND End Of Life (123915) 53 / tcp Low
internal | explicit | unauth dns

ISC Bind version 9.8.1 has surpassed its EOL date.

Product Has Reached End-of-Life Status (104220) 80 / tcp Low
internal | explicit | unauth http

Version 2.2.22 of the Apache Web Server has reached end-of-life status.

PHP End of Life (112906) 80 / tcp Low
internal | explicit | unauth http

Version 5.3.10 of PHP has reached end-of-life status.

Apache Tomcat End of Life (113012) 8080 / tcp Low
internal | explicit | unauth http

Apache Tomcat 6.0.35 has reached end-of-life status.

SSL Connection: SSL Version 3 Enabled (128440) 110 / tcp Low
internal | explicit | unauth pop3

Server supports SSL version 3

SSL Connection: SSL Version 3 Enabled (128440) 143 / tcp Low
internal | explicit | unauth imap

Server supports SSL version 3

SSL Connection: SSL Version 3 Enabled (128440) 443 / tcp Low
internal | explicit | unauth http (ssl)

Server supports SSL version 3

SSL Connection: SSL Version 3 Enabled (128440) 993 / tcp Low
internal | explicit | unauth imap (ssl)

Server supports SSL version 3

ISC BIND End Of Life (123915) 53 / udp Low
internal | explicit | unauth dns

ISC Bind version 9.8.1 has surpassed its EOL date.

SSL Connection: SSL Version 3 Enabled (128440) 995 / tcp Low
internal | explicit | unauth pop3 (ssl)

Server supports SSL version 3

Product Has Reached End-of-Life Status (104220) 443 / tcp Low
internal | explicit | unauth http (ssl)

Version 2.2.22 of the Apache Web Server has reached end-of-life status.

PHP End of Life (112906) 443 / tcp Low
internal | explicit | unauth http (ssl)

Version 5.3.10 of PHP has reached end-of-life status.

Samba End of Life (117557) 139 / tcp Low
internal | explicit | unauth smb

Samba 3.6.3 has reached end-of-life status.

SSL Connection: Sweet32 Vulnerability (121110) 110 / tcp Trivial
internal | explicit | unauth pop3

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110) 995 / tcp Trivial
internal | explicit | unauth pop3 (ssl)

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110) 143 / tcp Trivial
internal | explicit | unauth imap

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110) 443 / tcp Trivial
internal | explicit | unauth http (ssl)

[Large data section omitted]

SMB Null Session Authentication (101373) 139 / tcp Trivial
internal | recon | unauth smb

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110) 993 / tcp Trivial
internal | explicit | unauth imap (ssl)

[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	143 / tcp imap	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	143 / tcp imap	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	110 / tcp pop3	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	110 / tcp pop3	Trivial

	[Large data section omitted]	
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal** | **explicit** | **unauth**	993 / tcp imap (ssl)	Trivial
	[Large data section omitted]	
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Trivial
	[Large data section omitted]	
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal** | **explicit** | **unauth**	143 / tcp imap	Trivial
	[Large data section omitted]	
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal** | **explicit** | **unauth**	995 / tcp pop3 (ssl)	Trivial
	[Large data section omitted]	
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal** | **explicit** | **unauth**	110 / tcp pop3	Trivial
	[Large data section omitted]	
SSL Connection: TLS Compression Enabled (112280) **internal** | **explicit** | **unauth**	995 / tcp pop3 (ssl)	Trivial
	TLS Supports DEFLATE compression	
SSL Certificate: Chain Contains Weak RSA Keys (104022) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Trivial
	Inadequate Certificate Key Size: 1024	
SSL Connection: TLS Compression Enabled (112280) **internal** | **explicit** | **unauth**	993 / tcp imap (ssl)	Trivial
	TLS Supports DEFLATE compression	

SSL Connection: Anonymous (non-authenticated) Key-Agreement Protocols Permitted (122162) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
[Large data section omitted]		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
[Large data section omitted]		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
Server supports TLS version 1.0		
SSL Certificate: Expired Certificate Date (103615) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Date Appears Invalid: Jun 20 17:48:02 2013 GMT to Jun 20 17:48:02 2014 GMT		
SMB Native LanMan Version (100092) **internal | recon | unauth**	139 / tcp smb	Trivial
LAN Manager: Samba 3.6.3 Domain: WORKGROUP OS: Unix		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		
Default Apache Tomcat Webpage Detected (117554) **internal | recon | unauth**	8080 / tcp http	Trivial
Default Apache Tomcat 6 webpage detected		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	110 / tcp pop3	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	143 / tcp imap	Trivial

	Server supports TLS version 1.0

SSL Connection: Weak Ciphers Enabled (103617) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial

	[Large data section omitted]

TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial

	Server supports TLS version 1.0

UBUNTU F

IP: 192.168.67.55
Asset name: UBUNTU
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
http	80 / tcp
pop3	110 / tcp
netbios-ns	137 / udp
smb	139 / tcp
imap	143 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity

Easily Guessable SSH Credentials (104120) 22 / tcp Critical
internal | explicit | unauth ssh

successfully logged in with username: user, password: user

SMB Security Signatures Not Required (104188) 139 / tcp Low
internal | explicit | unauth smb

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

Phpinfo.php System Information Disclosure (100403) 80 / tcp Low
internal | explicit | unauth http

[Large data section omitted]

SMB Null Session Authentication (101373) 139 / tcp Trivial
internal | recon | unauth smb

It was possible to log into the remote host using a NULL session.

Content Security Policy Missing (148043) 80 / tcp Trivial
internal | explicit | unauth http

Missing Content Security Policy.

Web Server Default Error Page Detected (128223) 80 / tcp Trivial
internal | explicit | unauth http

[Large data section omitted]

SMB Native LanMan Version (100092) 139 / tcp Trivial
internal | recon | unauth smb

LAN Manager: Samba 4.3.8-Ubuntu
Domain: WORKGROUP
OS: Windows 6.1

UBUNTU-4-1320-1 F

IP: 192.168.67.58
Asset name: UBUNTU-4-1320-1
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp

telnet	23 / tcp
smtp	25 / tcp
http	80 / tcp
netbios-ns	137 / udp
smb	139 / tcp
snmp	161 / udp
http (ssl)	443 / tcp
mysql	3306 / tcp
postgresql (ssl)	5432 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Emerson Avocent Default SSH Credentials (118921) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
logged in with default credentials admin/avocent		
SSH Accepts Any Login (104178) **internal** | **explicit** | **unauth**	22 / tcp ssh	Medium
logged in with guest/guest ssh server appears to accept *ANY* login		
NetBIOS Shares Accessible (100870) **internal** | **explicit** | **unauth**	139 / tcp smb	Medium
NetBIOS Shares: dbfolder-serverlist, Home, uk-comp-classified, hs-engg-docs, sj-comp-employee-info, sj-comp-prod, pg-comp-itoperations, surfacepro, Public, ny-hr-comp, sj-comp-sales-prov, sncfile-server, sj-comp-print, homes, nyserver-finance, pg-comp-designing-repository, hs-comp-memory, to-comp-finance-olpghs, to-comp-vlan-info, sj-comp-helpdesk-support, sj-comp-dev, hrdbfolder, sj-comp-medicals		
SNMP Default Communities (100149) **internal** | **explicit** | **unauth**	161 / udp snmp	Medium

public

SMB Writeable Directories (104477)

internal | **explicit** | **unauth**

139 / tcp
smb

Medium

Writeable Directories
Share name 'Home':
\
Share name 'Public':
\

NetBIOS Shares With Everyone/Full-Control Permissions (104589)

internal | **explicit** | **unauth**

139 / tcp
smb

Low

NetBIOS Everyone Accessible Shares: Home (READ/WRITE), Public (READ/WRITE)

OpenSSL AES-NI CBC Padding Oracle Attack (119367)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

server accepts bad padding

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | **explicit** | **unauth**

25 / tcp
smtp

Low

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | **explicit** | **unauth**

5432 / tcp
postgresql (ssl)

Low

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - SSLv3
RC4-SHA - TLSv1
RC4-SHA - TLSv1.1
RC4-SHA - TLSv1.2

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

[Large data section omitted]

SSL Connection: RSA Export Grade Cipher FREAK Vulnerability (117845)

internal | **explicit** | **unauth**

25 / tcp
smtp

Low

[Large data section omitted]

SSL Connection: TLS Diffie-Hellman Export Cipher Downgrade Logjam Vulnerability (117846)

internal | **explicit** | **unauth**

25 / tcp
smtp

Low

EXP-EDH-RSA-DES-CBC-SHA - TLSv1
EXP-EDH-RSA-DES-CBC-SHA - TLSv11
EXP-EDH-RSA-DES-CBC-SHA - TLSv12

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SMB Security Signatures Not Required (104188)

internal | **explicit** | **unauth**

139 / tcp
smb

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

PHP End of Life (112906)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

Version 5.5.3 of PHP has reached end-of-life status.

Anonymous FTP Enabled (101362)

internal | **explicit** | **unauth**

21 / tcp
ftp

Low

anonymous

SSL Connection: SSL Version 3 Enabled (128440)

internal | **explicit** | **unauth**

25 / tcp
smtp

Low

Server supports SSL version 3

Ubuntu End of Life (117365)

internal | **explicit** | **unauth**

N/A / tcp
unknown

Low

Ubuntu 13.10 has reached end-of-life status.

SSL Connection: SSL Version 3 Enabled (128440)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

Server supports SSL version 3

SMTP Server EXPN/VRFY (100876)

internal | **explicit** | **unauth**

25 / tcp
smtp

Low

VRFY root: 252 2.0.0 root

SMB User Enumeration (113348)

internal | explicit | unauth

139 / tcp
smb

Low

[Large data section omitted]

SSL Connection: SSL Version 3 Enabled (128440)

internal | explicit | unauth

5432 / tcp
postgresql (ssl)

Low

Server supports SSL version 3

PHP End of Life (112906)

internal | explicit | unauth

80 / tcp
http

Low

Version 5.5.3 of PHP has reached end-of-life status.

Samba End of Life (117557)

internal | explicit | unauth

139 / tcp
smb

Low

Samba 3.6.18 has reached end-of-life status.

SMB Null Session Authentication (101373)

internal | recon | unauth

139 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

5432 / tcp
postgresql (ssl)

Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

25 / tcp
smtp

Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

5432 / tcp
postgresql (ssl)

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - SSLv3
RC4-SHA - TLSv1
RC4-SHA - TLSv1.1
RC4-SHA - TLSv1.2

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)
internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | explicit | unauth

25 / tcp
smtp

Trivial

[Large data section omitted]

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)
internal | explicit | unauth

25 / tcp
smtp

Trivial

Weak Signature Algorithm: SHA-1

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)
internal | explicit | unauth

5432 / tcp
postgresql (ssl)

Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)
internal | explicit | unauth

5432 / tcp
postgresql (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)
internal | explicit | unauth

25 / tcp
smtp

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)
internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

[Large data section omitted]

TLS Connection: TLS Version 1.0 Enabled (125641)
internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.0

SSL Connection: Weak Ciphers Enabled (103617) internal | explicit | unauth	25 / tcp smtp	Trivial
[Large data section omitted]		
SSL Certificate: Outdated Version (104020) internal | explicit | unauth	443 / tcp http (ssl)	Trivial
Outdated SSL Certificate Version: 1		
TLS Connection: TLS Version 1.0 Enabled (125641) internal | explicit | unauth	25 / tcp smtp	Trivial
Server supports TLS version 1.0		
SSL Connection: Anonymous (non-authenticated) Key-Agreement Protocols Permitted (122162) internal | explicit | unauth	25 / tcp smtp	Trivial
[Large data section omitted]		
SMB Native LanMan Version (100092) internal | recon | unauth	139 / tcp smb	Trivial
LAN Manager: Samba 3.6.18 Domain: WORKGROUP OS: Unix		
TLS Connection: TLS Version 1.0 Enabled (125641) internal | explicit | unauth	5432 / tcp postgresql (ssl)	Trivial
Server supports TLS version 1.0		

WINXP-ORACLE F

IP: 192.168.67.62
Asset name: WINXP-ORACLE
Operating system: Windows XP
Asset type: Client

Protocol	Service
telnet	23 / tcp
http	80 / tcp
netbios-ns	137 / udp
smb	445 / tcp

msrdp	3389 / tcp
vnc	5900 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS08-067 Microsoft Windows Server Service Stack Overflow (Network Check) (103802) **internal | explicit | unauth**	445 / tcp smb	Critical
MS08-067		
MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831) **internal | explicit | unauth**	3389 / tcp msrdp	Critical
Target asset is missing the patch for CVE-2019-0708: 03 00 00 09 02 f0 80 21 80 ....!.		
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal | explicit | unauth**	445 / tcp smb	Critical
This asset is missing the MS17-010 patch. Vulnerable Response: ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D.... 00 00 00 00 00 00 00 00 01 08 06 00 01 18 06 0d .... 00 00 00 ...		
Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST 11/18 - Patch Applied		
Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT remediated on 5/24		
Easily Guessable Telnet Credentials (111915) **internal | explicit | unauth**	23 / tcp telnet	High
[Large data section omitted]		

MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735)

3389 / tcp
msrdp

High

internal | explicit | unauth

Vulnerable to MS12-020:

```
03 00 00 0f 02 f0 80 3e 00 00 03 03 ed 03 ed .......>.......
```

Web Server Directory Traversal (100905)

80 / tcp
http

High

internal | explicit | unauth

[Large data section omitted]

Apache Win32 Directory Traversal (101929)

80 / tcp
http

High

internal | explicit | unauth

[Large data section omitted]

Apache Chunked Encoding Buffer Overflow (101470)

80 / tcp
http

High

internal | explicit | unauth

Apache chunked encoding buffer overflow

Microsoft Windows XP End of Life (113789)

N/A / tcp
unknown

High

internal | explicit | unauth

Support has ended for Windows XP. This host should be immediately upgraded.

MS09-001 SMB Remote Code Execution (Network Check) (103879)

445 / tcp
smb

Medium

internal | explicit | unauth

MS09-001

MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133)

445 / tcp
smb

Medium

internal | explicit | unauth

MS10-012 Weak NTLM Session Key Detected: (bdc80fae22b7cf64)

Web Server Directory Indexing Enabled (101049)

80 / tcp
http

Low

internal | explicit | unauth

Directory Indexing Enabled:
192.168.67.62:80:
/icons

MS09-048 Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities (104048)

445 / tcp
smb

Low

internal | explicit | unauth

MS09-048: TCP/IP DoS Detected

Apache Range Header Denial Of Service (117860)

internal | **explicit** | **unauth**

80 / tcp
http

Low

Webserver returned: 206 Partial Content

Webserver Expect Header Allows Cross-Site Scripting (104910)

internal | **explicit** | **unauth**

80 / tcp
http

Low

[Large data section omitted]

VNC Weak Password Encryption (101410)

internal | **explicit** | **unauth**

5900 / tcp
vnc

Low

VNC Authentication security type supported

SMB Security Signatures Not Required (104188)

internal | **explicit** | **unauth**

445 / tcp
smb

Low

SMBv1 NTLM signatures are not required

HTTP Host Header Value Reflection (128596)

internal | **explicit** | **unauth**

80 / tcp
http

Low

/cgi-bin/ : <A HREF="/">vm.frontline.cloud</A>
/error/ : <A HREF="/">vm.frontline.cloud</A>

Product Has Reached End-of-Life Status (104220)

internal | **explicit** | **unauth**

80 / tcp
http

Low

Version 2.0.35 of the Apache Web Server has reached end-of-life status.

Apache Manual Page Information Leak (103390)

internal | **explicit** | **unauth**

80 / tcp
http

Low

Apache 2.0 documentation page detected.

Apache Default Start Page (103388)

internal | **recon** | **unauth**

80 / tcp
http

Low

Unconfigured Apache server detected

SMB Null Session Authentication (101373)

internal | **recon** | **unauth**

445 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

Remote Desktop Protocol Allows Man in the Middle (117858)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)

HTTP TRACE/TRACK Method Enabled (117856) **internal | explicit | unauth**	80 / tcp http	Trivial
Not Applicable		
Microsoft RDP Network Level Authentication Disabled (128925) **internal | recon | unauth**	3389 / tcp msrdp	Trivial
NLA not enabled on target asset		
SMB Native LanMan Version (100092) **internal | recon | unauth**	445 / tcp smb	Trivial
LAN Manager: Windows 2000 LAN Manager Domain: WORKGROUP OS: Windows 5.1		

Bobby's Computer — F

IP: 192.168.67.66
Asset name: Bobby's Computer
Operating system: Debian 9 Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: user, password: user		
Debian End of Life (134009) **internal | explicit | unauth**	22 / tcp ssh	Low
Debian 9.0 has reached end-of-life status.		

192.168.67.66	F

IP: 192.168.67.66
Asset name: 192.168.67.66
Operating system: Debian 9 Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
iax2	4569 / udp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
successfully logged in with username: user, password: user		
Debian End of Life (134009) **internal** | **explicit** | **unauth**	22 / tcp ssh	Low
Debian 9.0 has reached end-of-life status.		

192.168.67.68	F

IP: 192.168.67.68
Asset name: 192.168.67.68
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp

unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
successfully logged in with username: root, password: password		
Content Security Policy Missing (148043) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial
Missing Content Security Policy.		
Web Server Default Error Page Detected (128223) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial
[Large data section omitted]		

192.168.67.69

F

IP: 192.168.67.69
Asset name: 192.168.67.69
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
telnet	23 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity

Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: admin, password: admin		
Unix Server Common Password (100151) **internal | explicit | unauth**	23 / tcp telnet	Critical
[Large data section omitted]		

WIN7WSUS

F

IP: 192.168.67.72
Asset name: WIN7WSUS
Operating system: Windows 7 Enterprise
Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal | explicit | unauth**	445 / tcp smb	Critical

This asset is missing the MS17-010 patch.

Vulnerable Response:

```
ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D....
00 00 00 00 00 00 00 00 00 08 06 00 00 08 06 0d ................
00 00 00 ...
```

Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST
11/18 - Patch Applied

Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT
remediated on 5/24

Microsoft Windows 7 End of Life (131864)

internal | explicit | unauth

N/A / tcp
unknown

High

Support has ended for Windows 7. This host should be immediately upgraded.

SMB Security Signatures Not Required (104188)

internal | explicit | unauth

445 / tcp
smb

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

SMB Null Session Authentication (101373)

internal | recon | unauth

445 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

SMB Native LanMan Version (100092)

internal | recon | unauth

445 / tcp
smb

Trivial

LAN Manager: Windows 7 Enterprise 6.1
Domain: SR
OS: Windows 7 Enterprise 7601 Service Pack 1

Asset Comments and Notes

Analyst Comment | Paris Stone (paris.stone@digitaldefense.com) | Thursday, March 29, 2018 8:59 AM CDT
Jim has to remediate this.

192.168.67.80 F

IP: 192.168.67.80
Asset name: 192.168.67.80
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: root, password: root		
Phpinfo.php System Information Disclosure (100403) **internal | explicit | unauth**	80 / tcp http	Low
[Large data section omitted]		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		

COMPUTER

F

IP: 192.168.67.81
Asset name: COMPUTER
Operating system: Windows Server 2008
Asset type: Server

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

MS09-050 Microsoft Windows SMB2 Command Execution Vulnerabilities (Network Check) (104045)

445 / tcp
smb

Critical

internal | explicit | unauth

MS09-050

MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051)

445 / tcp
smb

Critical

internal | explicit | unauth

This asset is missing the MS17-010 patch.

```
Vulnerable Response:
ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D....
00 00 00 00 00 00 00 00 05 18 06 00 02 10 06 0d ................
00 00 00 ...
```

Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST
11/18 - Patch Applied

Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT
remediated on 5/24

Microsoft Windows Server 2008 End of Life (131869)

N/A / tcp
unknown

High

internal | explicit | unauth

Support has ended for Windows Server 2008. This host should be immediately upgraded.

MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133)

445 / tcp
smb

Medium

internal | explicit | unauth

MS10-012 Weak NTLM Session Key Detected: (c5551c58c6b55303)

MS11-020: SMB Transaction Parsing Vulnerability (Network Check) (104422)

445 / tcp
smb

Medium

internal | explicit | unauth

ms11-020

SMB Security Signatures Not Required (104188)

445 / tcp
smb

Low

internal | explicit | unauth

SMBv1 NTLM signatures are not required

Microsoft Windows Service Pack Outdated (104065)

445 / tcp
smb

Low

internal | explicit | unauth

Windows 2008 Service Pack 2 is not installed

SMB Null Session Authentication (101373) **internal | recon | unauth**	445 / tcp smb	Trivial

It was possible to log into the remote host using a NULL session.

SMB Native LanMan Version (100092) **internal | recon | unauth**	445 / tcp smb	Trivial

LAN Manager: Windows Server (R) 2008 Standard without Hyper-V 6.0
Domain: WORKGROUP
OS: Windows Server (R) 2008 Standard without Hyper-V 6001 Service Pack 1

UBUNTU-4-1320-1 F

IP: 192.168.67.89
Asset name: UBUNTU-4-1320-1
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp
telnet	23 / tcp
smtp	25 / tcp
http	80 / tcp
netbios-ns	137 / udp
smb	139 / tcp
snmp	161 / udp
http (ssl)	443 / tcp
mysql	3306 / tcp
postgresql (ssl)	5432 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Emerson Avocent Default SSH Credentials (118921) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
logged in with default credentials admin/avocent		
SSH Accepts Any Login (104178) **internal** | **explicit** | **unauth**	22 / tcp ssh	Medium
logged in with user/user ssh server appears to accept *ANY* login		
NetBIOS Shares Accessible (100870) **internal** | **explicit** | **unauth**	139 / tcp smb	Medium
NetBIOS Shares: ny-hr-comp, sj-comp-medicals, Public, uk-comp-classified, pg-comp-designing-repository, surfacepro, dbfolder-serverlist, sj-comp-dev, sncfile-server, to-comp-vlan-info, nyserver-finance, hrdbfolder, pg-comp-itoperations, sj-comp-print, sj-comp-sales-prov, sj-comp-employee-info, hs-comp-memory, Home, sj-comp-helpdesk-support, sj-comp-prod, homes, hs-engg-docs, to-comp-finance-olpghs		
SNMP Default Communities (100149) **internal** | **explicit** | **unauth**	161 / udp snmp	Medium
public		
SMB Writeable Directories (104477) **internal** | **explicit** | **unauth**	139 / tcp smb	Medium
Writeable Directories Share name 'Home': \\ Share name 'Public': \\		
NetBIOS Shares With Everyone/Full-Control Permissions (104589) **internal** | **explicit** | **unauth**	139 / tcp smb	Low
NetBIOS Everyone Accessible Shares: Public (READ/WRITE), Home (READ/WRITE)		
OpenSSL AES-NI CBC Padding Oracle Attack (119367) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Low
server accepts bad padding		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	5432 / tcp postgresql (ssl)	Low

```
Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - SSLv3
RC4-SHA - TLSv1
RC4-SHA - TLSv1.1
RC4-SHA - TLSv1.2
```

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

25 / tcp
smtp

Low

internal | **explicit** | **unauth**

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

443 / tcp
http (ssl)

Low

internal | **explicit** | **unauth**

[Large data section omitted]

SSL Connection: RSA Export Grade Cipher FREAK Vulnerability (117845)

25 / tcp
smtp

Low

internal | **explicit** | **unauth**

[Large data section omitted]

SSL Connection: TLS Diffie-Hellman Export Cipher Downgrade Logjam Vulnerability (117846)

25 / tcp
smtp

Low

internal | **explicit** | **unauth**

```
EXP-EDH-RSA-DES-CBC-SHA - TLSv1
EXP-EDH-RSA-DES-CBC-SHA - TLSv11
EXP-EDH-RSA-DES-CBC-SHA - TLSv12
```

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843)

443 / tcp
http (ssl)

Low

internal | **explicit** | **unauth**

```
This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1
```

SMB Security Signatures Not Required (104188)

139 / tcp
smb

Low

internal | **explicit** | **unauth**

```
SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required
```

Anonymous FTP Enabled (101362)

21 / tcp
ftp

Low

internal | **explicit** | **unauth**

```
anonymous
```

PHP End of Life (112906) **internal | explicit | unauth**	443 / tcp http (ssl)	Low

Version 5.5.3 of PHP has reached end-of-life status.

SMB User Enumeration (113348) **internal | explicit | unauth**	139 / tcp smb	Low

[Large data section omitted]

Ubuntu End of Life (117365) **internal | explicit | unauth**	N/A / tcp unknown	Low

Ubuntu 13.10 has reached end-of-life status.

PHP End of Life (112906) **internal | explicit | unauth**	80 / tcp http	Low

Version 5.5.3 of PHP has reached end-of-life status.

Samba End of Life (117557) **internal | explicit | unauth**	139 / tcp smb	Low

Samba 3.6.18 has reached end-of-life status.

SSL Connection: SSL Version 3 Enabled (128440) **internal | explicit | unauth**	443 / tcp http (ssl)	Low

Server supports SSL version 3

SSL Connection: SSL Version 3 Enabled (128440) **internal | explicit | unauth**	5432 / tcp postgresql (ssl)	Low

Server supports SSL version 3

SMTP Server EXPN/VRFY (100876) **internal | explicit | unauth**	25 / tcp smtp	Low

VRFY root: 252 2.0.0 root

SSL Connection: SSL Version 3 Enabled (128440) **internal | explicit | unauth**	25 / tcp smtp	Low

Server supports SSL version 3

SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	5432 / tcp postgresql (ssl)	Trivial

[Large data section omitted]

SMB Null Session Authentication (101373) **internal | recon | unauth**	139 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
[Large data section omitted]		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	25 / tcp smtp	Trivial
[Large data section omitted]		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	5432 / tcp postgresql (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	25 / tcp smtp	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	25 / tcp smtp	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	5432 / tcp postgresql (ssl)	Trivial
SSL connection supports the following SSL/TLS RC4 ciphers: RC4-SHA - SSLv3 RC4-SHA - TLSv1 RC4-SHA - TLSv1.1 RC4-SHA - TLSv1.2		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Weak Signature Algorithm: SHA-1		

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

5432 / tcp
postgresql (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

25 / tcp
smtp

Trivial

[Large data section omitted]

SSL Connection: Anonymous (non-authenticated) Key-Agreement Protocols Permitted (122162)

internal | explicit | unauth

25 / tcp
smtp

Trivial

[Large data section omitted]

SSL Connection: Weak Ciphers Enabled (103617)

internal | explicit | unauth

25 / tcp
smtp

Trivial

[Large data section omitted]

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

25 / tcp
smtp

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

5432 / tcp
postgresql (ssl)

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.0

SMB Native LanMan Version (100092)

internal | recon | unauth

139 / tcp
smb

Trivial

LAN Manager: Samba 3.6.18
Domain: WORKGROUP
OS: Unix

SSL Certificate: Outdated Version (104020) internal | explicit | unauth	443 / tcp http (ssl)	Trivial

Outdated SSL Certificate Version: 1

YYY-BSERVER01	F

IP: 192.168.67.91
Asset name: YYY-BSERVER01
Operating system: CentOS
Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp
telnet	23 / tcp
smtp	25 / tcp
http	80 / tcp
rpcbind	111 / tcp
rpcbind	111 / udp
smb	139 / tcp
snmp	161 / udp
http (ssl)	443 / tcp
mysql	3306 / tcp
mysql	3307 / tcp
ajp	8009 / tcp
http	8080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Emerson Avocent Default SSH Credentials (118921) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
logged in with default credentials admin/avocent		
Samba IsKnownPipename Remote Code Execution (122062) **internal** | **explicit** | **unauth**	139 / tcp smb	Critical
This asset is missing the CVE-2017-7494 patch Payload: nirv64.so Share: Public Physical path: /usr/test/nirv64.so Successful Exploitation: Successfully retreived touch file		
Easily Guessable MySQL Credentials (104829) **internal** | **explicit** | **unauth**	3306 / tcp mysql	High
[Large data section omitted]		
Apache Tomcat "Ghostcat" AJP Local File Inclusion and RCE (132639) **internal** | **explicit** | **unauth**	8009 / tcp ajp	High
[Large data section omitted]		
SSH Accepts Any Login (104178) **internal** | **explicit** | **unauth**	22 / tcp ssh	Medium
logged in with user/user ssh server appears to accept *ANY* login		
NetBIOS Shares Accessible (100870) **internal** | **explicit** | **unauth**	139 / tcp smb	Medium
NetBIOS Shares: homes, Public, Home		
SNMP Default Communities (100149) **internal** | **explicit** | **unauth**	161 / udp snmp	Medium
public		
Web Server Directory Indexing Enabled (101049) **internal** | **explicit** | **unauth**	80 / tcp http	Low

Directory Indexing Enabled:
192.168.67.91:80:
/images
/style

Web Server Directory Indexing Enabled (101049)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

Directory Indexing Enabled:
192.168.67.91:443:
/images
/style

SSH Protocol 1 Enabled (100561)

internal | **explicit** | **unauth**

22 / tcp
ssh

Low

Supported versions: 2.0 1.5 1.33

NetBIOS Shares With Everyone/Full-Control Permissions (104589)

internal | **explicit** | **unauth**

139 / tcp
smb

Low

NetBIOS Everyone Accessible Shares: homes (READ/WRITE), Public (READ/WRITE), Home (READ/WRITE)

OpenSSL AES-NI CBC Padding Oracle Attack (119367)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

server accepts bad padding

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

[Large data section omitted]

Slowloris Resource Depletion And Denial Of Service (117854)

internal | **explicit** | **unauth**

8080 / tcp
http

Low

The webserver appears to be vulnerable to a resource exhaustion attack.

SMB Security Signatures Not Required (104188)

internal | **explicit** | **unauth**

139 / tcp
smb

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

Anonymous FTP Enabled (101362)

internal | **explicit** | **unauth**

21 / tcp
ftp

Low

anonymous

SMTP Server EXPN/VRFY (100876)

internal | **explicit** | **unauth**

25 / tcp
smtp

Low

	VRFY root: 252 2.0.0 root

OpenSSL End of Life (123917) **internal | explicit | unauth**	80 / tcp http	Low
	OpenSSL 1.0.1 has reached end-of-life status.	
PHP End of Life (112906) **internal | explicit | unauth**	80 / tcp http	Low
	Version 5.4.16 of PHP has reached end-of-life status.	
SSL Connection: SSL Version 3 Enabled (128440) **internal | explicit | unauth**	443 / tcp http (ssl)	Low
	Server supports SSL version 3	
OpenSSL End of Life (123917) **internal | explicit | unauth**	443 / tcp http (ssl)	Low
	OpenSSL 1.0.1 has reached end-of-life status.	
PHP End of Life (112906) **internal | explicit | unauth**	443 / tcp http (ssl)	Low
	Version 5.4.16 of PHP has reached end-of-life status.	
SMB User Enumeration (113348) **internal | explicit | unauth**	139 / tcp smb	Low
	[Large data section omitted]	
SMB Null Session Authentication (101373) **internal | recon | unauth**	139 / tcp smb	Trivial
	It was possible to log into the remote host using a NULL session.	
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
	[Large data section omitted]	
RPC Portmap Service (100505) **internal | explicit | unauth**	111 / udp rpcbind	Trivial
	Not Applicable	

RPC Portmap Service (100505)

internal | **explicit** | **unauth**

111 / tcp
rpcbind

Trivial

Not Applicable

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Trivial

[Large data section omitted]

Apache Server Header Information Disclosure (123916)

internal | **recon** | **unauth**

80 / tcp
http

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 SVN/1.7.14

Apache Server Header Information Disclosure (123916)

internal | **recon** | **unauth**

443 / tcp
http (ssl)

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.1e-fips PHP/5.4.16 SVN/1.7.14

SSL Certificate: Outdated Version (104020)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Trivial

Outdated SSL Certificate Version: 1

SMB Native LanMan Version (100092)

internal | **recon** | **unauth**

139 / tcp
smb

Trivial

LAN Manager: Samba 4.1.1
Domain: MYGROUP
OS: Unix

Default Apache Tomcat Webpage Detected (117554)

internal | **recon** | **unauth**

8080 / tcp
http

Trivial

Default Apache Tomcat webpage detected

TLS Connection: TLS Version 1.0 Enabled (125641) internal | explicit | unauth	443 / tcp http (ssl)	Trivial
Server supports TLS version 1.0		

192.168.67.92 F

IP: 192.168.67.92
Asset name: 192.168.67.92
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) internal | explicit | unauth	22 / tcp ssh	Critical
successfully logged in with username: root, password: root		
Phpinfo.php System Information Disclosure (100403) internal | explicit | unauth	80 / tcp http	Low
[Large data section omitted]		
WordPress Unsupported Version (128586) internal | explicit | unauth	80 / tcp http	Low
Detected unsupported WordPress version: 4.0.6		
Web Server Default Error Page Detected (128223) internal | explicit | unauth	80 / tcp http	Trivial
[Large data section omitted]		

192.168.67.98 F

IP: 192.168.67.98
Asset name: 192.168.67.98
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
http	9090 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: root, password: root		

Asset Comments and Notes
Comment | John Stahmann (john.stahmann@helpsystems.com) | Wednesday, March 25, 2020 12:48 PM CDT This is a web server
Comment | John Stahmann (john.stahmann@helpsystems.com) | Friday, Feb. 21, 2020 9:34 AM CST MacBook Pro

BASEWIN2K8SR2 F

IP: 192.168.67.102
Asset name: BASEWIN2K8SR2
Operating system: Windows Platform
Asset type: Client

Protocol	Service
msrpc	135 / tcp

msrdp	3389 / tcp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Critical
Target asset is missing the patch for CVE-2019-0708: 03 00 00 09 02 f0 80 21 80 ....!.		
MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	High
Vulnerable to MS12-020: 03 00 00 0f 02 f0 80 3e 00 00 03 03 ed 03 ed ....>.......		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1		
SSL Connection: Sweet32 Vulnerability (121110) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1: DES-CBC3-SHA		
Remote Desktop Protocol Allows Man in the Middle (117858) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
Weak Signature Algorithm: SHA-1		

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: AES128-SHA

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

Microsoft RDP Network Level Authentication Disabled (128925)

internal | recon | unauth

3389 / tcp
msrdp

Trivial

NLA not enabled on target asset

S1-WIN10-WKGP

F

IP: 192.168.67.244
Asset name: S1-WIN10-WKGP
Operating system: Windows 10 Enterprise
Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
msrdp	3389 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal | explicit | unauth**	445 / tcp smb	Critical
This asset is missing the MS17-010 patch. Vulnerable Response: ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D.... 00 00 00 00 00 00 00 00 03 a8 06 00 01 60 bf a9 ....\`.. 00 00 00 ...		
Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST 11/18 - Patch Applied		
Windows 10 End of Life (125528) **internal | explicit | unauth**	N/A / tcp unknown	High
Windows 10 version 1507 has reached end-of-life status		
MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756) **internal | explicit | unauth**	135 / tcp msrpc	Medium
This asset permits binding to samr pipe using auth level Connect. Response from asset: 02 . 22 00 00 c0 "... Responding port: 49414		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.2 RC4-SHA - TLSv1.2		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	445 / tcp smb	Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

SMB Null Session Authentication (101373)

internal | recon | unauth

445 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.2:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: ECDHE-RSA-AES256-SHA

SMB Native LanMan Version (100092)

internal | recon | unauth

445 / tcp
smb

Trivial

LAN Manager: Windows 10 Enterprise 6.3
Domain: WRKGRP1
OS: Windows 10 Enterprise 10240

TLS Connection: TLS Version 1.0 Enabled (125641) | 3389 / tcp msrdp | Trivial

internal | explicit | unauth

Server supports TLS version 1.0

WIN7WSUS F

IP: 192.168.68.55
Asset name: WIN7WSUS
Operating system: Windows 7 Enterprise
Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal | explicit | unauth**	445 / tcp smb	Critical

This asset is missing the MS17-010 patch.

Vulnerable Response:

```
ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D....
00 00 00 00 00 00 00 00 00 00 08 06 00 00 08 45 2e ..............E.
00 00 00 ...
```

Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST
11/18 - Patch Applied

Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT
remediated on 5/24

Microsoft Windows 7 End of Life (131864) **internal | explicit | unauth**	N/A / tcp unknown	High
Support has ended for Windows 7. This host should be immediately upgraded.		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	445 / tcp smb	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SMB Null Session Authentication (101373) **internal | recon | unauth**	445 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		
SMB Native LanMan Version (100092) **internal | recon | unauth**	445 / tcp smb	Trivial
LAN Manager: Windows 7 Enterprise 6.1 Domain: SR OS: Windows 7 Enterprise 7601 Service Pack 1		

Asset Comments and Notes

Analyst Comment | John Stahmann (john.stahmann@helpsystems.com) | Thursday, Aug. 19, 2021 12:37 PM CDT
These are detectives, and will have funky stuff on them!

192.168.68.65 F

IP: 192.168.68.65
Asset name: 192.168.68.65
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) internal | explicit | unauth	22 / tcp ssh	Critical
successfully logged in with username: admin, password: admin		
Content Security Policy Missing (148043) internal | explicit | unauth	80 / tcp http	Trivial
Missing Content Security Policy.		
Web Server Default Error Page Detected (128223) internal | explicit | unauth	80 / tcp http	Trivial
[Large data section omitted]		

192.168.68.66 F

IP: 192.168.68.66
Asset name: 192.168.68.66
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) internal | explicit | unauth	22 / tcp ssh	Critical
successfully logged in with username: root, password: root		
Phpinfo.php System Information Disclosure (100403) internal | explicit | unauth	80 / tcp http	Low

	[Large data section omitted]	
Content Security Policy Missing (148043) **internal | explicit | unauth**	80 / tcp http	Trivial
	Missing Content Security Policy.	
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
	[Large data section omitted]	

192.168.68.70 F

IP: 192.168.68.70
Asset name: 192.168.68.70
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
http	9090 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: root, password: root		
Content Security Policy Missing (148043) **internal | explicit | unauth**	80 / tcp http	Trivial
Missing Content Security Policy.		

192.168.68.70 F

IP: 192.168.68.70
Asset name: 192.168.68.70
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
http	9090 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
successfully logged in with username: root, password: root		
Content Security Policy Missing (148043) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial
Missing Content Security Policy.		

BASEWIN2K8SR2 F

IP: 192.168.68.73
Asset name: BASEWIN2K8SR2
Operating system: Windows Platform
Asset type: Client

Protocol	Service
msrpc	135 / tcp
msrdp	3389 / tcp

unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Critical
Target asset is missing the patch for CVE-2019-0708: 03 00 00 09 02 f0 80 21 80 ....!.		
MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	High
Vulnerable to MS12-020: 03 00 00 0f 02 f0 80 3e 00 00 03 03 ed 03 ed ....>.......		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1		
SSL Connection: Sweet32 Vulnerability (121110) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1: DES-CBC3-SHA		
Remote Desktop Protocol Allows Man in the Middle (117858) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1		

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: AES128-SHA

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

Microsoft RDP Network Level Authentication Disabled (128925)

internal | recon | unauth

3389 / tcp
msrdp

Trivial

NLA not enabled on target asset

Asset Comments and Notes

Analyst Comment | John Stahmann (john.stahmann@helpsystems.com) | Thursday, Aug. 19, 2021 12:37 PM CDT
These are detectives, and will have funky stuff on them!

192.168.68.88 F

IP: 192.168.68.88
Asset name: 192.168.68.88
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) internal | explicit | unauth	22 / tcp ssh	Critical
successfully logged in with username: root, password: password		

192.168.68.91 F

IP: 192.168.68.91
Asset name: 192.168.68.91
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
telnet	23 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) internal | explicit | unauth	22 / tcp ssh	Critical
successfully logged in with username: admin, password: admin		
Unix Server Common Password (100151) internal | explicit | unauth	23 / tcp telnet	Critical
[Large data section omitted]		

192.168.68.93 F

IP: 192.168.68.93
Asset name: 192.168.68.93
Operating system: Ubuntu Linux

Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
	successfully logged in with username: root, password: root	
Phpinfo.php System Information Disclosure (100403) **internal | explicit | unauth**	80 / tcp http	Low
	[Large data section omitted]	
WordPress Unsupported Version (128586) **internal | explicit | unauth**	80 / tcp http	Low
	Detected unsupported WordPress version: 4.0.6	
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
	[Large data section omitted]	

WINXP-ORACLE F

IP: 192.168.68.98
Asset name: WINXP-ORACLE
Operating system: Windows XP
Asset type: Client

Protocol	Service

telnet	23 / tcp
netbios-ns	137 / udp
smb	445 / tcp
msrdp	3389 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS08-067 Microsoft Windows Server Service Stack Overflow (Network Check) (103802) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
MS08-067		
MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Critical
Target asset is missing the patch for CVE-2019-0708: 03 00 00 09 02 f0 80 21 80 ....!.		
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
This asset is missing the MS17-010 patch. Vulnerable Response: ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D.... 00 00 00 00 00 00 00 00 03 18 06 00 02 88 e1 c8 .... 00 00 00 ...		
Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST 11/18 - Patch Applied		
Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT remediated on 5/24		

MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735)

internal | explicit | unauth

3389 / tcp
msrdp

High

Vulnerable to MS12-020:

```
03 00 00 0f 02 f0 80 3e 00 00 03 03 ed 03 ed .......>.......
```

Microsoft Windows XP End of Life (113789)

internal | explicit | unauth

N/A / tcp
unknown

High

Support has ended for Windows XP. This host should be immediately upgraded.

MS09-001 SMB Remote Code Execution (Network Check) (103879)

internal | explicit | unauth

445 / tcp
smb

Medium

MS09-001

MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133)

internal | explicit | unauth

445 / tcp
smb

Medium

MS10-012 Weak NTLM Session Key Detected: (52c7c3e5f4596db4)

MS09-048 Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities (104048)

internal | explicit | unauth

445 / tcp
smb

Low

MS09-048: TCP/IP DoS Detected

SMB Security Signatures Not Required (104188)

internal | explicit | unauth

445 / tcp
smb

Low

SMBv1 NTLM signatures are not required

SMB Null Session Authentication (101373)

internal | recon | unauth

445 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

Remote Desktop Protocol Allows Man in the Middle (117858)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)

SMB Native LanMan Version (100092)

internal | recon | unauth

445 / tcp
smb

Trivial

```
LAN Manager: Windows 2000 LAN Manager
Domain: WORKGROUP
OS: Windows 5.1
```

Microsoft RDP Network Level Authentication Disabled (128925) **internal | recon | unauth**	3389 / tcp msrdp	Trivial

NLA not enabled on target asset

Asset Comments and Notes

Analyst Comment | John Stahmann (john.stahmann@helpsystems.com) | Thursday, Aug. 19, 2021 12:37 PM CDT
These are detectives, and will have funky stuff on them!

BUFF-HEARTBLEED F

IP: 192.168.68.101
Asset name: BUFF-HEARTBLEED
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
http	80 / tcp
pop3	110 / tcp
netbios-ns	137 / udp
smb	139 / tcp
imap	143 / tcp
http (ssl)	443 / tcp
imap (ssl)	993 / tcp
pop3 (ssl)	995 / tcp
jdwp	8000 / tcp
http	8080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	143 / tcp imap	Critical
[Large data section omitted]		
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	110 / tcp pop3	Critical
[Large data section omitted]		
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	995 / tcp pop3 (ssl)	Critical
[Large data section omitted]		
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	993 / tcp imap (ssl)	Critical
[Large data section omitted]		
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Critical
[Large data section omitted]		
NetBIOS Shares Accessible (100870) **internal** | **explicit** | **unauth**	139 / tcp smb	Medium
NetBIOS Accessible Shares: myshare (READ/WRITE)		
Java Debugging Port Accessible (104527) **internal** | **explicit** | **unauth**	8000 / tcp jdwp	Medium
Java Debug Wire Protocol (Reference Implementation) version 1.6 JVM Debug Interface version 1.2 JVM version 1.6.0_27 (OpenJDK Client VM, mixed mode, sharing)1.6.0_27OpenJDK Client VM		
SMB Writeable Directories (104477) **internal** | **explicit** | **unauth**	139 / tcp smb	Medium
Writeable Directories Share name 'myshare': \		

Web Server Directory Indexing Enabled (101049)

80 / tcp
http

Low

internal | explicit | unauth

Directory Indexing Enabled:
192.168.68.101:80:

/keys

SSL Connection: Server Appears Vulnerable to ChangeCipherSpec Injection (115134)

993 / tcp
imap (ssl)

Low

internal | explicit | unauth

Host does not reject early change cipher spec using TLSv1.2
Host does not reject early change cipher spec using TLSv1.1
Host does not reject early change cipher spec using TLSv1
Host does not reject early change cipher spec using SSLv3

SSL Connection: Server Appears Vulnerable to ChangeCipherSpec Injection (115134)

443 / tcp
http (ssl)

Low

internal | explicit | unauth

Host does not reject early change cipher spec using TLSv1.1
Host does not reject early change cipher spec using TLSv1
Host does not reject early change cipher spec using SSLv3

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

995 / tcp
pop3 (ssl)

Low

internal | explicit | unauth

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

110 / tcp
pop3

Low

internal | explicit | unauth

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

143 / tcp
imap

Low

internal | explicit | unauth

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

993 / tcp
imap (ssl)

Low

internal | explicit | unauth

[Large data section omitted]

Slowloris Resource Depletion And Denial Of Service (117854)

8080 / tcp
http

Low

internal | explicit | unauth

The webserver appears to be vulnerable to a resource exhaustion attack.

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

[Large data section omitted]

SSL Connection: RSA Export Grade Cipher FREAK Vulnerability (117845)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

[Large data section omitted]

SSL Connection: TLS Diffie-Hellman Export Cipher Downgrade Logjam Vulnerability (117846)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

EXP-EDH-RSA-DES-CBC-SHA - TLSv1
EXP-EDH-RSA-DES-CBC-SHA - TLSv11
EXP-EDH-RSA-DES-CBC-SHA - TLSv12

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843)

internal | **explicit** | **unauth**

993 / tcp
imap (ssl)

Low

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843)

internal | **explicit** | **unauth**

995 / tcp
pop3 (ssl)

Low

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SMB Security Signatures Not Required (104188)

internal | **explicit** | **unauth**

139 / tcp
smb

Low

SMBv1 NTLM signatures are not required

PHP End of Life (112906)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

Version 5.3.10 of PHP has reached end-of-life status.

SSL Connection: SSL Version 3 Enabled (128440)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

Server supports SSL version 3

ISC BIND End Of Life (123915)

internal | **explicit** | **unauth**

53 / udp
dns

Low

ISC Bind version 9.8.1 has surpassed its EOL date.

SSL Connection: SSL Version 3 Enabled (128440)

internal | **explicit** | **unauth**

143 / tcp
imap

Low

Server supports SSL version 3

Product Has Reached End-of-Life Status (104220)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Low

Version 2.2.22 of the Apache Web Server has reached end-of-life status.

ISC BIND End Of Life (123915)

internal | **explicit** | **unauth**

53 / tcp
dns

Low

ISC Bind version 9.8.1 has surpassed its EOL date.

Apache Tomcat End of Life (113012)

internal | **explicit** | **unauth**

8080 / tcp
http

Low

Apache Tomcat 6.0.35 has reached end-of-life status.

SSL Connection: SSL Version 3 Enabled (128440)

internal | **explicit** | **unauth**

993 / tcp
imap (ssl)

Low

Server supports SSL version 3

SMB User Enumeration (113348)

internal | **explicit** | **unauth**

139 / tcp
smb

Low

```
Users for domain 'BUFF-HEARTBLEED':
nobody
superman
batman
cisco
buff
bill
admin
```

Samba End of Life (117557)
internal | explicit | unauth

139 / tcp
smb

Low

Samba 3.6.3 has reached end-of-life status.

PHP End of Life (112906)
internal | explicit | unauth

80 / tcp
http

Low

Version 5.3.10 of PHP has reached end-of-life status.

Product Has Reached End-of-Life Status (104220)
internal | explicit | unauth

80 / tcp
http

Low

Version 2.2.22 of the Apache Web Server has reached end-of-life status.

Ubuntu End of Life (117365)
internal | explicit | unauth

N/A / tcp
unknown

Low

Ubuntu 12.04 has reached end-of-life status.

SSL Connection: SSL Version 3 Enabled (128440)
internal | explicit | unauth

995 / tcp
pop3 (ssl)

Low

Server supports SSL version 3

SSL Connection: SSL Version 3 Enabled (128440)
internal | explicit | unauth

110 / tcp
pop3

Low

Server supports SSL version 3

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth

143 / tcp
imap

Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth

110 / tcp
pop3

Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth

995 / tcp
pop3 (ssl)

Trivial

[Large data section omitted]

SMB Null Session Authentication (101373)
internal | recon | unauth

139 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth
993 / tcp
imap (ssl)
Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth
443 / tcp
http (ssl)
Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | explicit | unauth
993 / tcp
imap (ssl)
Trivial

[Large data section omitted]

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)
internal | explicit | unauth
995 / tcp
pop3 (ssl)
Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | explicit | unauth
995 / tcp
pop3 (ssl)
Trivial

[Large data section omitted]

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)
internal | explicit | unauth
110 / tcp
pop3
Trivial

Weak Signature Algorithm: SHA-1

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)
internal | explicit | unauth
143 / tcp
imap
Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | explicit | unauth
143 / tcp
imap
Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | explicit | unauth
110 / tcp
pop3
Trivial

[Large data section omitted]

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)
internal | explicit | unauth
443 / tcp
http (ssl)
Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
[Large data section omitted]		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
[Large data section omitted]		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
[Large data section omitted]		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	110 / tcp pop3	Trivial
[Large data section omitted]		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	143 / tcp imap	Trivial
[Large data section omitted]		
SSL Connection: TLS Compression Enabled (112280) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
TLS Supports DEFLATE compression		
SSL Connection: TLS Compression Enabled (112280) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
TLS Supports DEFLATE compression		

SSL Certificate: Chain Contains Weak RSA Keys (104022) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Inadequate Certificate Key Size: 1024		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	110 / tcp pop3	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	110 / tcp pop3	Trivial
Server supports TLS version 1.1		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
Server supports TLS version 1.1		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
Server supports TLS version 1.1		
Default Apache Tomcat Webpage Detected (117554) **internal | recon | unauth**	8080 / tcp http	Trivial
Default Apache Tomcat 6 webpage detected		
SSL Connection: Anonymous (non-authenticated) Key-Agreement Protocols Permitted (122162) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial

[Large data section omitted]

Web Server Default Error Page Detected (128223)
internal | explicit | unauth
443 / tcp
http (ssl)
Trivial

[Large data section omitted]

TLS Connection: TLS Version 1.0 Enabled (125641)
internal | explicit | unauth
443 / tcp
http (ssl)
Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)
internal | explicit | unauth
443 / tcp
http (ssl)
Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)
internal | explicit | unauth
143 / tcp
imap
Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)
internal | explicit | unauth
143 / tcp
imap
Trivial

Server supports TLS version 1.1

SMB Native LanMan Version (100092)
internal | recon | unauth
139 / tcp
smb
Trivial

LAN Manager: Samba 3.6.3
Domain: WORKGROUP
OS: Unix

SSL Connection: Weak Ciphers Enabled (103617)
internal | explicit | unauth
443 / tcp
http (ssl)
Trivial

[Large data section omitted]

SSL Certificate: Expired Certificate Date (103615)
internal | explicit | unauth
443 / tcp
http (ssl)
Trivial

Date Appears Invalid: Jun 20 17:48:02 2013 GMT to Jun 20 17:48:02 2014 GMT

192.168.68.113 F

IP: 192.168.68.113
Asset name: 192.168.68.113
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
successfully logged in with username: root, password: password		
Web Server Default Error Page Detected (128223) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial
[Large data section omitted]		

COMPUTER F

IP: 192.168.68.215
Asset name: COMPUTER
Operating system: Windows Server 2008
Asset type: Server

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS09-050 Microsoft Windows SMB2 Command Execution Vulnerabilities (Network Check) (104045) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
MS09-050		
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
This asset is missing the MS17-010 patch. Vulnerable Response: ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D.... 00 00 00 00 00 00 00 00 01 a0 06 00 00 78 ff b3 ....x.. 00 00 00 ...		
Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST 11/18 - Patch Applied		
Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT remediated on 5/24		
Microsoft Windows Server 2008 End of Life (131869) **internal** | **explicit** | **unauth**	N/A / tcp unknown	High
Support has ended for Windows Server 2008. This host should be immediately upgraded.		
MS11-020: SMB Transaction Parsing Vulnerability (Network Check) (104422) **internal** | **explicit** | **unauth**	445 / tcp smb	Medium
ms11-020		
MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133) **internal** | **explicit** | **unauth**	445 / tcp smb	Medium
MS10-012 Weak NTLM Session Key Detected: (1addd43314f505ee)		
SMB Security Signatures Not Required (104188) **internal** | **explicit** | **unauth**	445 / tcp smb	Low
SMBv1 NTLM signatures are not required		

Vulnerability Title	Service(s)	Severity
Microsoft Windows Service Pack Outdated (104065) **internal | explicit | unauth**	445 / tcp smb	Low
Windows 2008 Service Pack 2 is not installed		
SMB Null Session Authentication (101373) **internal | recon | unauth**	445 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		
SMB Native LanMan Version (100092) **internal | recon | unauth**	445 / tcp smb	Trivial
LAN Manager: Windows Server (R) 2008 Standard without Hyper-V 6.0 Domain: WORKGROUP OS: Windows Server (R) 2008 Standard without Hyper-V 6001 Service Pack 1		

WIN10-1507 F

IP: 192.168.68.223
Asset name: WIN10-1507
Operating system: Windows 10 Enterprise
Asset type: Client

Protocol	Service
unknown	68 / udp
msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal | explicit | unauth**	445 / tcp smb	Critical

This asset is missing the MS17-010 patch.

Vulnerable Response:

```
ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D....
00 00 00 00 00 00 00 00 02 58 06 00 03 a8 45 2e .........X....E.
00 00 00 ...
```

Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST
11/18 - Patch Applied

Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT
remediated on 5/24

SMB Null Session Authentication (101373)

internal | recon | unauth

445 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

SMB Native LanMan Version (100092)

internal | recon | unauth

445 / tcp
smb

Trivial

LAN Manager: Windows 10 Enterprise 6.3
Domain: QA0
OS: Windows 10 Enterprise 10240

Asset Comments and Notes

Analyst Comment | John Stahmann (john.stahmann@helpsystems.com) | Thursday, Aug. 19, 2021 12:37 PM CDT
These are detectives, and will have funky stuff on them!

BUFF-HEARTBLEED

F

IP: 192.168.69.106
Asset name: BUFF-HEARTBLEED
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	21 / tcp
ssh	22 / tcp
unknown	25 / tcp
dns	53 / tcp
dns	53 / udp
unknown	68 / udp
http	80 / tcp

pop3	110 / tcp
ntp	123 / udp
netbios-ns	137 / udp
unknown	138 / udp
smb	139 / tcp
imap	143 / tcp
http (ssl)	443 / tcp
smb	445 / tcp
unknown	587 / tcp
imap (ssl)	993 / tcp
pop3 (ssl)	995 / tcp
unknown	5353 / udp
jdwp	8000 / tcp
http	8080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Critical
[Large data section omitted]		
SSL Connection: Server Vulnerable to Heartbleed Attack (113790) **internal** | **explicit** | **unauth**	993 / tcp imap (ssl)	Critical
[Large data section omitted]		

SSL Connection: Server Vulnerable to Heartbleed Attack (113790)

internal | **explicit** | **unauth**

995 / tcp
pop3 (ssl)

Critical

[Large data section omitted]

SSL Connection: Server Vulnerable to Heartbleed Attack (113790)

internal | **explicit** | **unauth**

143 / tcp
imap

Critical

[Large data section omitted]

SSL Connection: Server Vulnerable to Heartbleed Attack (113790)

internal | **explicit** | **unauth**

110 / tcp
pop3

Critical

[Large data section omitted]

NetBIOS Shares Accessible (100870)

internal | **explicit** | **unauth**

139 / tcp
smb

Medium

```
NetBIOS Accessible Shares: myshare (READ/WRITE)
```

Java Debugging Port Accessible (104527)

internal | **explicit** | **unauth**

8000 / tcp
jdwp

Medium

```
Java Debug Wire Protocol (Reference Implementation) version 1.6
JVM Debug Interface version 1.2
JVM version 1.6.0_27 (OpenJDK Client VM, mixed mode, sharing)1.6.0_27OpenJDK Client VM
```

SMB Writeable Directories (104477)

internal | **explicit** | **unauth**

139 / tcp
smb

Medium

```
Writeable Directories
Share name 'myshare':
\
```

Web Server Directory Indexing Enabled (101049)

internal | **explicit** | **unauth**

80 / tcp
http

Low

```
Directory Indexing Enabled:
192.168.69.106:80:

/keys
```

SSL Connection: Server Appears Vulnerable to ChangeCipherSpec Injection (115134)

internal | **explicit** | **unauth**

993 / tcp
imap (ssl)

Low

```
Host does not reject early change cipher spec using TLSv1.2
Host does not reject early change cipher spec using TLSv1.1
Host does not reject early change cipher spec using TLSv1
Host does not reject early change cipher spec using SSLv3
```

SSL Connection: Server Appears Vulnerable to ChangeCipherSpec Injection (115134) **internal | explicit | unauth**	443 / tcp http (ssl)	Low
Host does not reject early change cipher spec using TLSv1.1 Host does not reject early change cipher spec using TLSv1 Host does not reject early change cipher spec using SSLv3		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	443 / tcp http (ssl)	Low
[Large data section omitted]		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	993 / tcp imap (ssl)	Low
[Large data section omitted]		
Slowloris Resource Depletion And Denial Of Service (117854) **internal | explicit | unauth**	8080 / tcp http	Low
The webserver appears to be vulnerable to a resource exhaustion attack.		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Low
[Large data section omitted]		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	143 / tcp imap	Low
[Large data section omitted]		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	110 / tcp pop3	Low
[Large data section omitted]		
SSL Connection: RSA Export Grade Cipher FREAK Vulnerability (117845) **internal | explicit | unauth**	443 / tcp http (ssl)	Low
[Large data section omitted]		

SSL Connection: TLS Diffie-Hellman Export Cipher Downgrade Logjam Vulnerability (117846)

443 / tcp
http (ssl)

Low

internal | **explicit** | **unauth**

EXP-EDH-RSA-DES-CBC-SHA - TLSv1
EXP-EDH-RSA-DES-CBC-SHA - TLSv11
EXP-EDH-RSA-DES-CBC-SHA - TLSv12

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843)

443 / tcp
http (ssl)

Low

internal | **explicit** | **unauth**

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843)

993 / tcp
imap (ssl)

Low

internal | **explicit** | **unauth**

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability (117843)

995 / tcp
pop3 (ssl)

Low

internal | **explicit** | **unauth**

This server supports SSLv3 with CBC mode ciphers. The server's highest supported protocol: TLSv1.2
Server allows a client to connect with the lower protocol: TLSv1.1

SMB Security Signatures Not Required (104188)

139 / tcp
smb

Low

internal | **explicit** | **unauth**

SMBv1 NTLM signatures are not required

Product Has Reached End-of-Life Status (104220)

443 / tcp
http (ssl)

Low

internal | **explicit** | **unauth**

Version 2.2.22 of the Apache Web Server has reached end-of-life status.

PHP End of Life (112906)

443 / tcp
http (ssl)

Low

internal | **explicit** | **unauth**

Version 5.3.10 of PHP has reached end-of-life status.

SSL Connection: SSL Version 3 Enabled (128440)

443 / tcp
http (ssl)

Low

internal | **explicit** | **unauth**

Server supports SSL version 3

SSL Connection: SSL Version 3 Enabled (128440)

993 / tcp
imap (ssl)

Low

internal | **explicit** | **unauth**

Server supports SSL version 3

ISC BIND End Of Life (123915) 53 / udp Low

internal | explicit | unauth dns

ISC Bind version 9.8.1 has surpassed its EOL date.

Apache Tomcat End of Life (113012) 8080 / tcp Low

internal | explicit | unauth http

Apache Tomcat 6.0.35 has reached end-of-life status.

Product Has Reached End-of-Life Status (104220) 80 / tcp Low

internal | explicit | unauth http

Version 2.2.22 of the Apache Web Server has reached end-of-life status.

PHP End of Life (112906) 80 / tcp Low

internal | explicit | unauth http

Version 5.3.10 of PHP has reached end-of-life status.

SSL Connection: SSL Version 3 Enabled (128440) 143 / tcp Low

internal | explicit | unauth imap

Server supports SSL version 3

Ubuntu End of Life (117365) N/A / tcp Low

internal | explicit | unauth unknown

Ubuntu 12.04 has reached end-of-life status.

SSL Connection: SSL Version 3 Enabled (128440) 110 / tcp Low

internal | explicit | unauth pop3

Server supports SSL version 3

Samba End of Life (117557) 139 / tcp Low

internal | explicit | unauth smb

Samba 3.6.3 has reached end-of-life status.

ISC BIND End Of Life (123915) 53 / tcp Low

internal | explicit | unauth dns

ISC Bind version 9.8.1 has surpassed its EOL date.

SSL Connection: SSL Version 3 Enabled (128440) 995 / tcp Low

internal | explicit | unauth pop3 (ssl)

Server supports SSL version 3

SMB User Enumeration (113348)
internal | explicit | unauth
139 / tcp
smb
Low

Users for domain 'BUFF-HEARTBLEED':
nobody
superman
batman
cisco
buff
bill
admin

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth
110 / tcp
pop3
Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth
143 / tcp
imap
Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth
995 / tcp
pop3 (ssl)
Trivial

[Large data section omitted]

SMB Null Session Authentication (101373)
internal | recon | unauth
139 / tcp
smb
Trivial

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth
993 / tcp
imap (ssl)
Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth
443 / tcp
http (ssl)
Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | explicit | unauth
443 / tcp
http (ssl)
Trivial

[Large data section omitted]

SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	143 / tcp imap	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	143 / tcp imap	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	110 / tcp pop3	Trivial
[Large data section omitted]		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	110 / tcp pop3	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	110 / tcp pop3	Trivial

[Large data section omitted]		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	143 / tcp imap	Trivial
[Large data section omitted]		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
[Large data section omitted]		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
[Large data section omitted]		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
[Large data section omitted]		
SSL Connection: TLS Compression Enabled (112280) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
TLS Supports DEFLATE compression		
SSL Certificate: Chain Contains Weak RSA Keys (104022) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Inadequate Certificate Key Size: 1024		
SSL Connection: TLS Compression Enabled (112280) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
TLS Supports DEFLATE compression		
SSL Connection: Weak Ciphers Enabled (103617) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
[Large data section omitted]		
SSL Connection: Anonymous (non-authenticated) Key-Agreement Protocols Permitted (122162) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial

	[Large data section omitted]

Web Server Default Error Page Detected (128223) 443 / tcp Trivial
internal | explicit | unauth http (ssl)

[Large data section omitted]

TLS Connection: TLS Version 1.0 Enabled (125641) 443 / tcp Trivial
internal | explicit | unauth http (ssl)

Server supports TLS version 1.0

SSL Certificate: Expired Certificate Date (103615) 443 / tcp Trivial
internal | explicit | unauth http (ssl)

Date Appears Invalid: Jun 20 17:48:02 2013 GMT to Jun 20 17:48:02 2014 GMT

TLS Connection: TLS Version 1.0 Enabled (125641) 993 / tcp Trivial
internal | explicit | unauth imap (ssl)

Server supports TLS version 1.0

Default Apache Tomcat Webpage Detected (117554) 8080 / tcp Trivial
internal | recon | unauth http

Default Apache Tomcat 6 webpage detected

Web Server Default Error Page Detected (128223) 80 / tcp Trivial
internal | explicit | unauth http

[Large data section omitted]

TLS Connection: TLS Version 1.0 Enabled (125641) 143 / tcp Trivial
internal | explicit | unauth imap

Server supports TLS version 1.0

TLS Connection: TLS Version 1.0 Enabled (125641) 110 / tcp Trivial
internal | explicit | unauth pop3

Server supports TLS version 1.0

SMB Native LanMan Version (100092) 139 / tcp Trivial
internal | recon | unauth smb

LAN Manager: Samba 3.6.3
Domain: WORKGROUP
OS: Unix

TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
Server supports TLS version 1.0		

192.168.69.107

F

IP: 192.168.69.107
Asset name: 192.168.69.107
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: root, password: root		
Phpinfo.php System Information Disclosure (100403) **internal | explicit | unauth**	80 / tcp http	Low
[Large data section omitted]		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		

UBUNTU

F

IP: 192.168.69.110
Asset name: UBUNTU
Operating system: Ubuntu Linux

Asset type: Server

Protocol	Service
ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
http	80 / tcp
pop3	110 / tcp
netbios-ns	137 / udp
smb	139 / tcp
imap	143 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: user, password: user		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp smb	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SMB Null Session Authentication (101373) **internal | recon | unauth**	139 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		

Web Server Default Error Page Detected (128223) internal | explicit | unauth	80 / tcp http	Trivial
	[Large data section omitted]	
SMB Native LanMan Version (100092) internal | recon | unauth	139 / tcp smb	Trivial
	LAN Manager: Samba 4.3.8-Ubuntu Domain: WORKGROUP OS: Windows 6.1	

ATS-WIN7-2 F

IP: 192.168.69.112
Asset name: ATS-WIN7-2
Operating system: Windows 7 Enterprise
Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
msrdp	3389 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) internal | explicit | unauth	445 / tcp smb	Critical

This asset is missing the MS17-010 patch.

Vulnerable Response:

```
ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D....
00 00 00 00 00 00 00 00 00 08 06 00 00 08 23 9e .............#.
00 00 00 ...
```

Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST
11/18 - Patch Applied

Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT
remediated on 5/24

Threat Detected: Trojan Variant (126460)

N/A / tcp
unknown

Critical

internal | malware | Threat Scan auth

Detection: PWS:Win32/Zbot!GO (53/56)
Type: Trojan
Path: C:\Users\administrator\Downloads\invoice copy.exe
Description: Running Process
SHA1 Hash: 6fc3e57274f50cc26d7ff025fbc99c3e707e99d2
SHA256 Hash: add4d12bd245abd5f826128562b837fca84d7bd0af16f69606dfb0979568e45f
Analysis:
https://www.virustotal.com/file/add4d12bd245abd5f826128562b837fca84d7bd0af16f69606dfb0979568e45f/analysis/1478030373/

MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735)

3389 / tcp
msrdp

High

internal | explicit | unauth

Vulnerable to MS12-020:

```
03 00 00 0f 02 f0 80 3e 00 00 03 03 ed 03 ed .......>.......
```

Microsoft Windows 7 End of Life (131864)

N/A / tcp
unknown

High

internal | explicit | unauth

Support has ended for Windows 7. This host should be immediately upgraded.

MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133)

445 / tcp
smb

Medium

internal | explicit | unauth

MS10-012 Weak NTLM Session Key Detected: (f022ef249356635f)

MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756)

135 / tcp
msrpc

Medium

internal | explicit | unauth

This asset permits binding to samr pipe using auth level Connect.
Response from asset:

```
02 .

22 00 00 c0 "...
```

Responding port: 49154

Threat Scan: McAfee VirusScan Enterprise Definitions Outdated (126543)

N/A / tcp
unknown

Medium

internal | explicit | Threat Scan auth

Detected definition version: 2018/01/01 version 1089

Threat Scan: Windows Defender Disabled (127063) N/A / tcp Medium

internal | explicit | Threat Scan auth unknown

The Windows Defender service is not currently running.

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) 3389 / tcp Low

internal | explicit | unauth msrdp

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1

SMB Security Signatures Not Required (104188) 445 / tcp Low

internal | explicit | unauth smb

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

Microsoft Windows Service Pack Outdated (104065) 445 / tcp Low

internal | explicit | unauth smb

Windows 7 Service Pack 1 is not installed

SMB Null Session Authentication (101373) 445 / tcp Trivial

internal | recon | unauth smb

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110) 3389 / tcp Trivial

internal | explicit | unauth msrdp

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

Remote Desktop Protocol Allows Man in the Middle (117858) 3389 / tcp Trivial

internal | explicit | unauth msrdp

rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) 3389 / tcp Trivial

internal | explicit | unauth msrdp

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: AES128-SHA

SMB Native LanMan Version (100092)

internal | recon | unauth

445 / tcp
smb

Trivial

LAN Manager: Windows 7 Enterprise 6.1
Domain: ATS
OS: Windows 7 Enterprise 7600

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

Microsoft RDP Network Level Authentication Disabled (128925)

internal | recon | unauth

3389 / tcp
msrdp

Trivial

NLA not enabled on target asset

Asset Comments and Notes

Analyst Comment | John Stahmann (john.stahmann@helpsystems.com) | Wednesday, March 24, 2021 2:15 PM CDT
Comment

192.168.69.113 F

IP: 192.168.69.113
Asset name: 192.168.69.113
Operating system: Debian 9 Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp

http	80 / tcp
http	10000 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: user, password: user		
Phpinfo.php System Information Disclosure (100403) **internal | explicit | unauth**	80 / tcp http	Low
[Large data section omitted]		
Apache Manual Page Information Leak (103390) **internal | explicit | unauth**	80 / tcp http	Low
Apache 2.4 documentation page detected.		
HTTP Host Header Value Reflection (128596) **internal | explicit | unauth**	80 / tcp http	Low
/manual : an't connect to vm.frontline.cloud:80 (Bad hostnam		
Debian End of Life (134009) **internal | explicit | unauth**	22 / tcp ssh	Low
Debian 9.0 has reached end-of-life status.		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		

192.168.69.116 F

IP: 192.168.69.116
Asset name: 192.168.69.116

Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	21 / tcp
ssh	22 / tcp
http	80 / tcp
unknown	514 / udp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal | explicit | unauth**	22 / tcp ssh	Critical
successfully logged in with username: root, password: password		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		

192.168.69.125 F

IP: 192.168.69.125
Asset name: 192.168.69.125
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp

unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
successfully logged in with username: admin, password: admin		
Web Server Default Error Page Detected (128223) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial
[Large data section omitted]		

192.168.69.126	**F**

IP: 192.168.69.126
Asset name: 192.168.69.126
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
telnet	23 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Easily Guessable SSH Credentials (104120) **internal** | **explicit** | **unauth**	22 / tcp ssh	Critical
successfully logged in with username: admin, password: admin		

Unix Server Common Password (100151) **internal** | **explicit** | **unauth**	23 / tcp telnet	Critical
[Large data section omitted]		

ATS-WIN7-ENT64 F

IP: 192.168.69.245
Asset name: ATS-WIN7-ENT64
Operating system: Windows 7 Enterprise
Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
msrdp	3389 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Critical
Target asset is missing the patch for CVE-2019-0708: 03 00 00 09 02 f0 80 21 80 ....!.		
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
This asset is missing the MS17-010 patch. Vulnerable Response: ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D.... 00 00 00 00 00 00 00 00 00 08 06 00 00 08 23 9e ....#. 00 00 00 ...		

Acceptable Risk Note | Zvi Magnes (zvim@beyondsecurity.com) | Friday, Oct. 22, 2021 6:09 AM CDT
accepted

Comment | Troy Myers (troy.myers@digitaldefense.com) | Wednesday, Nov. 18, 2020 9:20 AM CST
11/18 - Patch Applied

Comment | Troy Myers (troy.myers@digitaldefense.com) | Tuesday, May 26, 2020 10:00 AM CDT
remediated on 5/24

Threat Detected: Trojan Variant (126460)

internal | malware | Threat Scan auth

N/A / tcp
unknown

Critical

Detection: Win.Trojan.Agent-551827 (34/68)
Type: Trojan
Path: C:\Windows\Temp\LIBjKSShsBtZM\metsvc.exe
Description: Running Process
SHA1 Hash: 7232bd42cd9d0725e7e0220052f4734fec91be7a
SHA256 Hash: fc512a7264fa6a546ab1f503c8bd8f11787ed23d05f3783a76d932b1722f8d70
Analysis:
https://www.virustotal.com/file/fc512a7264fa6a546ab1f503c8bd8f11787ed23d05f3783a76d932b1722f8d70/analysis/1542314810/

MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735)

internal | explicit | unauth

3389 / tcp
msrdp

High

Vulnerable to MS12-020:

03 00 00 0f 02 f0 80 3e 00 00 03 03 ed 03 ed ....>.......

Microsoft Windows 7 End of Life (131864)

internal | explicit | unauth

N/A / tcp
unknown

High

Support has ended for Windows 7. This host should be immediately upgraded.

MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133)

internal | explicit | unauth

445 / tcp
smb

Medium

MS10-012 Weak NTLM Session Key Detected: (02384852c04f6c28)

MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756)

internal | explicit | unauth

135 / tcp
msrpc

Medium

This asset permits binding to samr pipe using auth level Connect.
Response from asset:
02 .

22 00 00 c0 "...

Responding port: 49154

Threat Scan: Windows Defender Disabled (127063)

internal | explicit | Threat Scan auth

N/A / tcp
unknown

Medium

The Windows Defender service is not currently running.

Threat Scan: Antivirus Software Not Installed (126539) N/A / tcp Medium
internal | **explicit** | **Threat Scan auth** unknown

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) 3389 / tcp Low
internal | **explicit** | **unauth** msrdp

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1

SMB Security Signatures Not Required (104188) 445 / tcp Low
internal | **explicit** | **unauth** smb

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

Microsoft Windows Service Pack Outdated (104065) 445 / tcp Low
internal | **explicit** | **unauth** smb

Windows 7 Service Pack 1 is not installed

SMB Null Session Authentication (101373) 445 / tcp Trivial
internal | **recon** | **unauth** smb

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110) 3389 / tcp Trivial
internal | **explicit** | **unauth** msrdp

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

Remote Desktop Protocol Allows Man in the Middle (117858) 3389 / tcp Trivial
internal | **explicit** | **unauth** msrdp

rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) 3389 / tcp Trivial
internal | **explicit** | **unauth** msrdp

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1

SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
SSL connection supports the following SSLv3/TLSv1 CBC mode cipher: AES128-SHA - TLSv1 AES256-SHA - TLSv1 DES-CBC3-SHA - TLSv1 ECDHE-RSA-AES128-SHA - TLSv1 ECDHE-RSA-AES256-SHA - TLSv1 BEAST not mitigated: server ignores client order but prefers CBC mode ciphers Cipher used: AES128-SHA		
SMB Native LanMan Version (100092) **internal | recon | unauth**	445 / tcp smb	Trivial
LAN Manager: Windows 7 Enterprise 6.1 Domain: ATS OS: Windows 7 Enterprise 7600		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
Server supports TLS version 1.0		
Microsoft RDP Network Level Authentication Disabled (128925) **internal | recon | unauth**	3389 / tcp msrdp	Trivial
NLA not enabled on target asset		

Asset Comments and Notes

Comment | Hernan Torres (hernan.torres@helpsystems.com) | Wednesday, Dec. 7, 2022 9:57 AM CST
Movimiento Lateral y exposición

Analyst Comment | John Stahmann (john.stahmann@helpsystems.com) | Wednesday, Aug. 18, 2021 8:47 AM CDT
Cody, please get some AV on this device

ADMIN-PC F

IP: 192.168.100.78
Asset name: ADMIN-PC
Operating system: Windows 7
Asset type: Client

Protocol	Service

msrpc	135 / tcp
netbios-ns	137 / udp
smb	445 / tcp
msrdp	3389 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	N/A	Failure

Vulnerability Title	Service(s)	Severity
MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) (128831) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Critical
Target asset is missing the patch for CVE-2019-0708: 03 00 00 09 02 f0 80 21 80 ....!.		
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
This asset is missing the MS17-010 patch. Vulnerable Response: ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D.... 00 00 00 00 00 00 00 00 00 08 06 00 00 08 e4 12 .... 00 00 00 ...		
MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) (104735) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	High
Vulnerable to MS12-020: 03 00 00 0f 02 f0 80 3e 00 00 03 03 ed 03 ed ....>.......		
Microsoft Windows 7 End of Life (131864) **internal** | **explicit** | **unauth**	N/A / tcp unknown	High
Support has ended for Windows 7. This host should be immediately upgraded.		

MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756)

internal | **explicit** | **unauth**

135 / tcp
msrpc

Medium

```
This asset permits binding to samr pipe using auth level Connect.
Response from asset:
02 .

22 00 00 c0 "...

Responding port: 49186
```

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Low

```
Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
```

SMB Security Signatures Not Required (104188)

internal | **explicit** | **unauth**

445 / tcp
smb

Low

```
SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required
```

SMB Null Session Authentication (101373)

internal | **recon** | **unauth**

445 / tcp
smb

Trivial

```
It was possible to log into the remote host using a NULL session.
```

Remote Desktop Protocol Allows Man in the Middle (117858)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

```
rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)
```

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

```
Weak Signature Algorithm: SHA-1
```

SSL Connection: Sweet32 Vulnerability (121110)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

```
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA
```

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
ECDHE-RSA-AES256-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
DES-CBC3-SHA - TLSv1
AES256-SHA - TLSv1
AES128-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: AES128-SHA

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.2 Not Enabled (146258)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server does not support TLS version 1.2

Microsoft RDP Network Level Authentication Disabled (128925)

internal | recon | unauth

3389 / tcp
msrdp

Trivial

NLA not enabled on target asset

SSL Certificate: Expired Certificate Date (103615)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Date Appears Invalid: Oct 28 08:14:14 2018 GMT to Apr 29 08:14:14 2019 GMT

SMB Native LanMan Version (100092)

internal | recon | unauth

445 / tcp
smb

Trivial

LAN Manager: Windows 7 Ultimate 6.1
Domain: FREEFLY
OS: Windows 7 Ultimate 7601 Service Pack 1

CASH-F32CDFF50A F

IP: 192.168.100.80
Asset name: CASH-F32CDFF50A
Operating system: Windows XP
Asset type: Client

Protocol	Service
netbios-ns	137 / udp
smb	445 / tcp
postgresql	5432 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS08-067 Microsoft Windows Server Service Stack Overflow (Network Check) (103802) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
MS08-067		
MS17-010: SMB Remote Code Execution Vulnerability (Network Check) (122051) **internal** | **explicit** | **unauth**	445 / tcp smb	Critical
This asset is missing the MS17-010 patch. Vulnerable Response: ff 53 4d 42 25 05 02 00 c0 88 01 44 00 10 00 00 .SMB%......D.... 00 00 00 00 00 00 00 00 07 18 06 00 01 08 01 4d ....M 00 00 00 ...		
Microsoft Windows XP End of Life (113789) **internal** | **explicit** | **unauth**	N/A / tcp unknown	High
Support has ended for Windows XP. This host should be immediately upgraded.		
MS09-001 SMB Remote Code Execution (Network Check) (103879) **internal** | **explicit** | **unauth**	445 / tcp smb	Medium
MS09-001		
MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check) (104133) **internal** | **explicit** | **unauth**	445 / tcp smb	Medium

MS10-012 Weak NTLM Session Key Detected: (22d995435720c7ab)

MS09-048 Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities (104048)
445 / tcp
smb
Low

internal | explicit | unauth

MS09-048: TCP/IP DoS Detected

SMB Security Signatures Not Required (104188)
445 / tcp
smb
Low

internal | explicit | unauth

SMBv1 NTLM signatures are not required

SMB Null Session Authentication (101373)
445 / tcp
smb
Trivial

internal | recon | unauth

It was possible to log into the remote host using a NULL session.

SMB Native LanMan Version (100092)
445 / tcp
smb
Trivial

internal | recon | unauth

LAN Manager: Windows 2000 LAN Manager
Domain: WORKGROUP
OS: Windows 5.1

DESKTOP-17TP2JK D

IP: 10.0.0.98
Asset name: DESKTOP-17TP2JK
Operating system: Windows 10 Enterprise
Asset type: Client

Protocol	Service
smtp	25 / tcp
http	80 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
unknown (ssl)	277 / tcp
smb	445 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp

http	9700 / tcp
http	9702 / tcp
http	9703 / tcp
http	9708 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Success	N/A	Failure	Success

Authenticated Scan Credentials Used Successfully
OS: Tim's Win Cred **CIS:** Tim's Win Cred **Threatscan:** Tim's Win Cred

Vulnerability Title	Service(s)	Severity
MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Registry Entry Not Set (149637) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High
MS13_098: Microsoft Security Update is installed but the registry entry has not been set. Registry key incorrectly set: Software\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config		
MS22-JUN: Microsoft SQL Server Security Update (148996) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS22-JUN Vulnerable Path: C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\SQL2019\x64\microsoft.sqlserver.chainer.infrastructure.dll File Version: 15.0.4013.40 Fixed Version: 15.0.4236.7 Remediation KB(s): KB5014353,KB5014356		
Unquoted Windows Service Path Vulnerability (117555) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High
Service Name: ancoraDocs Input Service Unquoted Path: C:\Program Files (x86)\Ancora\ancoraDocs Online\InputService.exe		

MS21-JAN: Microsoft SQL Server Security Update (143780)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS21-JAN
Vulnerable Path: C:\Program Files\Microsoft SQL Server\150\Setup Bootstrap\SQL2019\x64\microsoft.sqlserver.chainer.infrastructure.dll
File Version: 15.0.4013.40
Fixed Version: 15.0.4083.2
Remediation KB(s): KB4583459,KB4583458

Threat Scan: Antivirus Software Not Installed (126539)

internal | explicit | Threat Scan auth

N/A / tcp
unknown

Medium

[Large data section omitted]

Threat Scan: Unsigned Software Processes (127839)

internal | explicit | Threat Scan auth

N/A / tcp
unknown

Medium

[Large data section omitted]

NetBIOS Shares With Everyone/Full-Control Permissions (104589)

internal | explicit | OS auth

445 / tcp
smb

Low

NetBIOS Everyone Writeable: MyEnvironmentXML (READ/WRITE)

Protocol Allows Authentication Over Clear Text (104798)

internal | explicit | unauth

25 / tcp
smtp

Low

smtp allows transmission of credentials in clear text

SMB Security Signatures Not Required (104188)

internal | explicit | unauth

445 / tcp
smb

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

SMB Null Session Authentication (101373)

internal | recon | unauth

445 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

277 / tcp
unknown (ssl)

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.2:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
ECDHE-RSA-AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
AES256-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
AES128-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

Content Security Policy Missing (148043)

internal | explicit | unauth

80 / tcp
http

Trivial

Missing Content Security Policy.

SMB Native LanMan Version (100092)

internal | recon | unauth

445 / tcp
smb

Trivial

LAN Manager: Windows 10 Enterprise 6.3
Domain: WORKGROUP
OS: Windows 10 Enterprise 19042

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

Link Local Multicast Name Resolution (LLMNR) Enabled (129962)

internal | recon | OS auth

N/A / tcp
unknown

Trivial

LLMNR is enabled

IPv6 Enabled (142306)

internal | explicit | OS auth

N/A / tcp
unknown

Trivial

IPv6 enabled on network interfaces with the following IPv4 addresses

10.0.0.98

10.1.1.24	D

IP: 10.1.1.24
Asset name: 10.1.1.24
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
OpenSSH 'ssh-agent' Double Free Vulnerability (144213) internal | potential | unauth	22 / tcp ssh	High
7.6p1		
OpenSSH 'scp' Command Evaluation Vulnerability (138013) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH scp Server Man-in-The-Middle Attack Vulnerability (127851) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH Sensitive Data Exposure Vulnerability (146710) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH 'auth-gss2.c' User Detection Vulnerability (126832) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		

OpenSSH User Enumeration Vulnerability (126863) **internal | potential | unauth**	22 / tcp ssh	Medium
	7.6p1	
OpenSSH Privilege Escalation Vulnerability (146711) **internal | potential | unauth**	22 / tcp ssh	Medium
	7.6p1	
OpenSSH Account Enumeration Vulnerability (126640) **internal | potential | unauth**	22 / tcp ssh	Medium
	7.6p1	
OpenSSH 'Observable Discrepancy' Man-in-the-Middle Vulnerability (137503) **internal | potential | unauth**	22 / tcp ssh	Medium
	7.6p1	
OpenSSH Missing Character Man-in-The-Middle Attack Vulnerability (127849) **internal | potential | unauth**	22 / tcp ssh	Medium
	7.6p1	
OpenSSH 'stderr' Man-in-The-Middle Attack Vulnerability (127850) **internal | potential | unauth**	22 / tcp ssh	Medium
	7.6p1	
OpenSSH Security Advisory (148395) **internal | potential | unauth**	22 / tcp ssh	Low
	7.6p1	
OpenSSH scp Client Access Bypass Vulnerability (127848) **internal | potential | unauth**	22 / tcp ssh	Low
	7.6p1	
ICMP Timestamp Request (150396) **internal | recon | unauth**	N/A / icmp unknown	Trivial
	icmp timestamp response	
IMPACT		**D**

IP: 10.27.34.7
Asset name: IMPACT
Operating system: Windows Platform
Asset type: Server

Protocol	Service
smtp	25 / tcp
pop3	110 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
imap	143 / tcp
unknown	445 / tcp
smtp	587 / tcp
msrdp	3389 / tcp
http (ssl)	8080 / tcp
http	9999 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Success	N/A	Failure	Success

Authenticated Scan Credentials Used Successfully
OS: MyRNA Azure **CIS:** MyRNA Azure **Threatscan:** MyRNA Azure

Vulnerability Title	Service(s)	Severity
MS22-JUL: Microsoft Windows Security Update (149222) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS22-JUL
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 10.0.22000.739
Fixed Version: 10.0.22000.795

MS22-JUN: Microsoft SQL Server Security Update (148996) N/A / tcp **High**
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS22-JUN
Vulnerable Path: C:\Program Files (x86)\Microsoft SQL Server\120\Setup Bootstrap\SQLServer2014\x86\microsoft.sqlserver.chainer.infrastructure.dll
File Version: 12.0.6024.0
Fixed Version: 12.0.6169.19
Remediation KB(s): KB5014164,KB5014165

MS19-JUL: Microsoft SQL Server Security Update (129105) N/A / tcp **High**
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS19-JUL
Vulnerable Path: C:\Program Files (x86)\Microsoft SQL Server\120\Setup Bootstrap\SQLServer2014\x86\microsoft.sqlserver.chainer.infrastructure.dll
File Version: 12.0.6024.0
Fixed Version: 12.0.6108.1
Remediation KB(s): KB4505419,KB4505422,KB4505218,KB4505217

MS20-FEB: Microsoft SQL Server Security Update (132519) N/A / tcp **High**
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS20-FEB
Vulnerable Path: C:\Program Files (x86)\Microsoft SQL Server\120\Setup Bootstrap\SQLServer2014\x86\microsoft.sqlserver.chainer.infrastructure.dll
File Version: 12.0.6024.0
Fixed Version: 12.0.6118.4
Remediation KB(s): KB4532095,KB4535288

MS21-JAN: Microsoft SQL Server Security Update (143780) N/A / tcp **Medium**
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS21-JAN
Vulnerable Path: C:\Program Files (x86)\Microsoft SQL Server\120\Setup Bootstrap\SQLServer2014\x86\microsoft.sqlserver.chainer.infrastructure.dll
File Version: 12.0.6024.0
Fixed Version: 12.0.6164.21
Remediation KB(s): KB4583462,KB4583463

Threat Scan: Unsigned Software Processes (127839) N/A / tcp **Medium**
internal | explicit | Threat Scan auth unknown

[Large data section omitted]

Protocol Allows Authentication Over Clear Text (104798) 143 / tcp **Low**
internal | explicit | unauth imap

imap allows transmission of credentials in clear text

Protocol Allows Authentication Over Clear Text (104798)

internal | **explicit** | **unauth**

110 / tcp
pop3

Low

pop3 allows transmission of credentials in clear text

Protocol Allows Authentication Over Clear Text (104798)

internal | **explicit** | **unauth**

587 / tcp
smtp

Low

smtp allows transmission of credentials in clear text

Protocol Allows Authentication Over Clear Text (104798)

internal | **explicit** | **unauth**

25 / tcp
smtp

Low

smtp allows transmission of credentials in clear text

SSL Connection: Sweet32 Vulnerability (121110)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
ECDHE-RSA-AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
AES256-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
AES128-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

Content Security Policy Missing (148043)

internal | **explicit** | **unauth**

9999 / tcp
http

Trivial

Missing Content Security Policy.

SSL Certificate: Chain Contains Weak RSA Keys (104022)

internal | **explicit** | **unauth**

8080 / tcp
http (ssl)

Trivial

Inadequate Certificate Key Size: 1024

SMB Native LanMan Version (100092)

internal | **recon** | **unauth**

139 / tcp
netbios

Trivial

LAN Manager: 10.0.22000.15
Domain: impact
OS: Windows 11 build 22000

TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial

Server supports TLS version 1.1

Link Local Multicast Name Resolution (LLMNR) Enabled (129962) **internal | recon | OS auth**	N/A / tcp unknown	Trivial

LLMNR is enabled

IPv6 Enabled (142306) **internal | explicit | OS auth**	N/A / tcp unknown	Trivial

IPv6 enabled on network interfaces with the following IPv4 addresses

33.0.0.6
10.27.34.7
10.27.34.7

cobaltstrike.internal.cloudapp.net D

IP: 10.27.34.69
Asset name: cobaltstrike.internal.cloudapp.net
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
http (ssl)	443 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
OpenSSH 'ssh-agent' Double Free Vulnerability (144213) **internal | potential | unauth**	22 / tcp ssh	High
7.6p1		
OpenSSH 'scp' Command Evaluation Vulnerability (138013) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH scp Server Man-in-The-Middle Attack Vulnerability (127851) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH 'auth-gss2.c' User Detection Vulnerability (126832) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH Sensitive Data Exposure Vulnerability (146710) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH User Enumeration Vulnerability (126863) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH Privilege Escalation Vulnerability (146711) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH Account Enumeration Vulnerability (126640) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH 'Observable Discrepancy' Man-in-the-Middle Vulnerability (137503) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		

OpenSSH Missing Character Man-in-The-Middle Attack Vulnerability (127849) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH 'stderr' Man-in-The-Middle Attack Vulnerability (127850) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH Security Advisory (148395) internal | potential | unauth	22 / tcp ssh	Low
7.6p1		
OpenSSH scp Client Access Bypass Vulnerability (127848) internal | potential | unauth	22 / tcp ssh	Low
7.6p1		

legendarykings.internal.cloudapp.net D

IP: 10.27.34.75
Asset name: legendarykings.internal.cloudapp.net
Operating system: Ubuntu Linux
Asset type: Client

Protocol	Service
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Apache httpd '2.2.32 2.4.24' Remote Segmentation Fault Vulnerability (290291) internal | potential | unauth	80 / tcp http	High

2.4.7		
Apache httpd '2.2.x before 2.2.33' and '2.4.x before 2.4.26' 'mod_ssl' subcomponent NULL pointer Vulnerability (290295) internal | potential | unauth	80 / tcp http	High
2.4.7		
Apache HTTP Server Security Update 2.4.51 (147293) internal | potential | unauth	80 / tcp http	High
2.4.7		
Apache HTTP Server 2.4.53 Security Release (148390) internal | potential | unauth	80 / tcp http	High
2.4.7		
Apache httpd '2.2.x before 2.2.33 and 2.4.x before 2.4.26' 'mod_mime' subcomponent Remote Read Vulnerability (290301) internal | potential | unauth	80 / tcp http	High
2.4.7		
Apache HTTP Server 'ap_get_basic_auth_pw' Authentication Bypass (290284) internal | potential | unauth	80 / tcp http	High
2.4.7		
Apache HTTP Server Security Update 2.4.48 (145498) internal | potential | unauth	80 / tcp http	High
2.4.7		
Apache HTTP Server 'mod_proxy_ftp' Uninitialized Memory Usage Vulnerability (133605) internal | potential | unauth	80 / tcp http	High
2.4.7		
Apache HTTP Server 'mod_http2' Module Denial of Service Vulnerability (282886) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server Security Update 2.4.49 (146396) internal | potential | unauth	80 / tcp http	Medium

2.4.7		
Apache HTTP Server 'mod_status' Module Race Condition (265518) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server Multiple Vulnerabilities (126218) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache httpd Digest Authorization Denial of Service (291127) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_auth_digest' Access Control Bypass Vulnerability (128444) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_rewrite' Redirect Vulnerability (133604) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server URL Redirect Vulnerability (129591) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server HTTP_PROXY Environment Variable Vulnerability (126237) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server HTTP Chunked Request Smuggling Attack (126232) **internal | potential | unauth**	80 / tcp http	Medium
2.4.7		
Apache HTTP Server Padding Oracle Vulnerability (288579) **internal | potential | unauth**	80 / tcp http	Medium

2.4.7		
Apache HTTP Server Digest Authentication Denial of Service (288580) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'cache_merge_headers_out' Function Denial of Service Vulnerability (126230) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache 'Optionsbleed' UAF Memory Leak (122625) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server ' mod_log_config' Denial of Service (263002) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server Response Splitting Vulnerability (288581) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'lua_websocket_read' Function Denial of Service Vulnerability (126231) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_session_cookie' Expiry Time Ignored Vulnerability (126276) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP "RequestHeader unset" Directive Bypass Vulnerability (126217) internal | potential | unauth	80 / tcp http	Medium
2.4.7		

Apache HTTP Server 'httpd' URL Normalization Inconsistency Vulnerability (128448) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_dav' Denial of Service (263007) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server winnt_accept Function Denial of Service (265505) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_cgid' Module Denial of Service (265538) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_cache_socache' Out of Bound Read Denial of Service Vulnerability (126242) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'ap_some_auth_required' Function Remote Access Restrictions Bypass Vulnerability (273795) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'mod_userdir' CRLF Injection Vulnerability (126838) internal | potential | unauth	80 / tcp http	Medium
2.4.7		
Apache HTTP Server 'deflate_in_filter' Function Denial of Service (265521) internal | potential | unauth	80 / tcp http	Medium
2.4.7		

Apache HTTP Server 'mod_lua' Access Restriction Bypass Vulnerability (269848)
internal | potential | unauth

80 / tcp
http

Medium

2.4.7

Apache HTTP Server 'mod_proxy' Module Denial of Service (265530)
internal | potential | unauth

80 / tcp
http

Medium

2.4.7

Apache HTTP Server 'mod_proxy' Cross-Site Scripting Vulnerability (129590)
internal | potential | unauth

80 / tcp
http

Medium

2.4.7

Apache HTTP Server mod_cluster Improper Input Validation Vulnerability (126238)
internal | potential | unauth

80 / tcp
http

Low

2.4.7

Content Security Policy Missing (148043)
internal | explicit | unauth

80 / tcp
http

Trivial

Missing Content Security Policy.

Web Server Default Error Page Detected (128223)
internal | explicit | unauth

80 / tcp
http

Trivial

[Large data section omitted]

WIN10VPN **D**

IP: 10.27.34.80
Asset name: WIN10VPN
Operating system: Windows 10 Pro
Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp

unknown	445 / tcp
msrdp	3389 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Success	N/A	Failure	Success

Authenticated Scan Credentials Used Successfully

OS: MyRNA Azure ACME
CIS: MyRNA Azure ACME
Threatscan: MyRNA Azure ACME

Vulnerability Title	Service(s)	Severity
MS21-DEC: Microsoft Windows Security Update (147272) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS21-DEC Vulnerable Path: C:\windows\system32\win32kfull.sys File Version: 10.0.19041.1320 Fixed Version: 10.0.19041.1387 Remediation KB(s): KB5008212		
MS22-MAY: Microsoft Windows Security Update (148572) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS22-MAY Vulnerable Path: C:\windows\system32\ntoskrnl.exe File Version: 10.0.19041.1348 Fixed Version: 10.0.19041.1706		
MS22-JUN: Microsoft Windows Security Update (148994) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS22-JUN Vulnerable Path: C:\windows\system32\ntoskrnl.exe File Version: 10.0.19041.1348 Fixed Version: 10.0.19041.1766		
MS22-APR: Microsoft Windows Security Update (148319) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS22-APR
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 10.0.19041.1348
Fixed Version: 10.0.19041.1645

MS22-JAN: Microsoft Windows Security Update (147420)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-JAN
Vulnerable Path: C:\windows\system32\win32kfull.sys
File Version: 10.0.19041.1320
Fixed Version: 10.0.19041.1466

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.52 (146565)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 93.0.961.52
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 95.0.1020.30 (146797)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 95.0.1020.30
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.44 (146376)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 93.0.961.44
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

MS22-FEB: Microsoft Windows Security Update (147753)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-FEB
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 10.0.19041.1348
Fixed Version: 10.0.19041.1526

MS22-JUL: Microsoft Windows Security Update (149222)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-JUL
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 10.0.19041.1348
Fixed Version: 10.0.19041.1826

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.47 (146377)

internal | explicit | OS auth

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 93.0.961.47
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 92.0.902.78 (146249)

internal | explicit | OS auth

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 92.0.902.78
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

MS22-MAR: Microsoft Internet Explorer Security Update (148036)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.19041.1320
Fixed Version: 11.0.19041.1566

MS22-MAR: Microsoft Windows Security Update (148037)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-MAR
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 10.0.19041.1348
Fixed Version: 10.0.19041.1586

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 103.0.1264.37 (149068)

internal | explicit | OS auth

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 103.0.1264.37
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 103.0.1264.44 (149202)

internal | explicit | OS auth

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 103.0.1264.44
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 102.0.1245.30 (148969)

internal | explicit | OS auth

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 102.0.1245.30
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 97.0.1072.55 (147417) **internal | explicit | OS auth**	N/A / tcp unknown	High

Installed version: 92.0.902.67
Vulnerable versions: all less than 97.0.1072.55
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.38 (146375) **internal | explicit | OS auth**	N/A / tcp unknown	High

Installed version: 92.0.902.67
Vulnerable versions: all less than 93.0.961.38
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 96.0.1054.29 (147105) **internal | explicit | OS auth**	N/A / tcp unknown	High

Installed version: 92.0.902.67
Vulnerable versions: all less than 96.0.1054.29
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 99.0.1150.46 (148265) **internal | explicit | OS auth**	N/A / tcp unknown	High

Installed version: 92.0.902.67
Vulnerable versions: all less than 99.0.1150.46
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 100.0.1185.44 (148439) **internal | explicit | OS auth**	N/A / tcp unknown	High

Installed version: 92.0.902.67
Vulnerable versions: all less than 100.0.1185.44
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 103.0.1264.49 (149201) **internal | explicit | OS auth**	N/A / tcp unknown	High

Installed version: 92.0.902.67
Vulnerable versions: all less than 103.0.1264.49
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 102.0.1245.41 (148970) **internal | explicit | OS auth**	N/A / tcp unknown	High
Installed version: 92.0.902.67 Vulnerable versions: all less than 102.0.1245.41 Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 98.0.1108.50 (148025) **internal | explicit | OS auth**	N/A / tcp unknown	High
Installed version: 92.0.902.67 Vulnerable versions: all less than 98.0.1108.50 Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 99.0.1150.55 (148267) **internal | explicit | OS auth**	N/A / tcp unknown	High
Installed version: 92.0.902.67 Vulnerable versions: all less than 99.0.1150.55 Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 101.0.1210.47 (148761) **internal | explicit | OS auth**	N/A / tcp unknown	High
Installed version: 92.0.902.67 Vulnerable versions: all less than 101.0.1210.47 Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 100.0.1185.36 (148266) **internal | explicit | OS auth**	N/A / tcp unknown	High
Installed version: 92.0.902.67 Vulnerable versions: all less than 100.0.1185.36 Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 101.0.1210.32 (148544) **internal | explicit | OS auth**	N/A / tcp unknown	High
Installed version: 92.0.902.67 Vulnerable versions: all less than 101.0.1210.32 Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		
Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 94.0.992.31 (146566) **internal | explicit | OS auth**	N/A / tcp unknown	High

Installed version: 92.0.902.67
Vulnerable versions: all less than 94.0.992.31
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 95.0.1020.40 (146924)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 95.0.1020.40
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 98.0.1108.55 (148026)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 98.0.1108.55
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 99.0.1150.30 (148024)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 99.0.1150.30
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 94.0.992.38 (146671)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 94.0.992.38
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 94.0.992.47 (146670)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 94.0.992.47
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 96.0.1054.57 (147257)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 96.0.1054.57
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 98.0.1108.43 (147751)

internal | explicit | OS auth

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 98.0.1108.43
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 100.0.1185.29 (148268)

internal | explicit | OS auth

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 100.0.1185.29
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 102.0.1245.39 (148968)

internal | explicit | OS auth

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 102.0.1245.39
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 97.0.1072.69 (147752)

internal | explicit | OS auth

N/A / tcp
unknown

High

Installed version: 92.0.902.67
Vulnerable versions: all less than 97.0.1072.69
Path: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

Windows 10 End of Life (125528)

internal | explicit | OS auth

N/A / tcp
unknown

High

Windows 10 version 2004 has reached end-of-life status

Threat Scan: Windows Defender Definitions Outdated (126741)

internal | explicit | Threat Scan auth

N/A / tcp
unknown

Medium

Definitions last updated: 09/24/2019 05:12:58
Detected definition version: 1.303.25.0

Threat Scan: Unsigned Software Processes (127839)

internal | explicit | Threat Scan auth

N/A / tcp
unknown

Medium

Process ID: 2548
Process Name: frontlinescan.exe
Parent ID: 708
Image Path: C:\Windows\frontlinescan.exe
SHA256 Hash: 119172238AEB3CA19F8A5E38644E26847421CD4A091C0AA13114D8D538094B04

MS22-MAY: Microsoft .NET Security Update (148574)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Low

Missing Microsoft Patch: MS22-MAY
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.data.dll
File Version: 4.8.4270.0
Fixed Version: 4.8.4455.0

SMB Security Signatures Not Required (104188)

internal | **explicit** | **unauth**

139 / tcp
netbios

Low

SMBv2 NTLM signatures are not required

SSL Connection: Sweet32 Vulnerability (121110)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1
AES256-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
AES128-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

SMB Native LanMan Version (100092)

internal | **recon** | **unauth**

139 / tcp
netbios

Trivial

LAN Manager: 10.0.19041.15
Domain: acme
OS: Windows 10 Build 19041

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

	Server supports TLS version 1.1

Link Local Multicast Name Resolution (LLMNR) Enabled (129962) **internal | recon | OS auth**	N/A / tcp unknown	Trivial
	LLMNR is enabled	
IPv6 Enabled (142306) **internal | explicit | OS auth**	N/A / tcp unknown	Trivial
	IPv6 enabled on network interfaces with the following IPv4 addresses 10.27.34.80 10.27.34.80	

juiceshop.internal.cloudapp.net — D

IP: 10.27.34.86
Asset name: juiceshop.internal.cloudapp.net
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
OpenSSH 'ssh-agent' Double Free Vulnerability (144213) **internal | potential | unauth**	22 / tcp ssh	High
7.6p1		
OpenSSH 'scp' Command Evaluation Vulnerability (138013) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		

OpenSSH scp Server Man-in-The-Middle Attack Vulnerability (127851) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH 'auth-gss2.c' User Detection Vulnerability (126832) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH Sensitive Data Exposure Vulnerability (146710) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH User Enumeration Vulnerability (126863) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH Privilege Escalation Vulnerability (146711) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH 'Observable Discrepancy' Man-in-the-Middle Vulnerability (137503) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH Account Enumeration Vulnerability (126640) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH Missing Character Man-in-The-Middle Attack Vulnerability (127849) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH 'stderr' Man-in-The-Middle Attack Vulnerability (127850) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		

OpenSSH scp Client Access Bypass Vulnerability (127848) internal | potential | unauth	22 / tcp ssh	Low
7.6p1		
Insecure HTML5 Cross Origin Request Policy (118119) internal | explicit | unauth	80 / tcp http	Low
[Large data section omitted]		

webapps.internal.cloudapp.net D

IP: 10.27.34.87
Asset name: webapps.internal.cloudapp.net
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Apache HTTP Server Internal Data Buffering Denial of Service Vulnerability (129589) internal | potential | unauth	80 / tcp http	High
2.4.29		
Apache HTTP Server Security Update 2.4.48 (145498) internal | potential | unauth	80 / tcp http	High
2.4.29		
Apache HTTP Server 2.4.53 Security Release (148390) internal | potential | unauth	80 / tcp http	High

2.4.29		
Apache HTTP Server Security Update 2.4.51 (147293) internal | potential | unauth	80 / tcp http	High
2.4.29		
Apache HTTP Server 'Module Scripts' Privilege Escalation Vulnerability (128443) internal | potential | unauth	80 / tcp http	High
2.4.29		
Apache HTTP Server 'mod_proxy_ftp' Uninitialized Memory Usage Vulnerability (133605) internal | potential | unauth	80 / tcp http	High
2.4.29		
OpenSSH 'ssh-agent' Double Free Vulnerability (144213) internal | potential | unauth	22 / tcp ssh	High
7.6p1		
OpenSSH 'scp' Command Evaluation Vulnerability (138013) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
Apache HTTP Server Security Update 2.4.49 (146396) internal | potential | unauth	80 / tcp http	Medium
2.4.29		
Apache HTTP Server Multiple Vulnerabilities (126218) internal | potential | unauth	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'mod_http2' Read-After-Free (CVE-2019-10082) (129592) internal | potential | unauth	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'mod_auth_digest' Access Control Bypass Vulnerability (128444) internal | potential | unauth	80 / tcp http	Medium

2.4.29		
OpenSSH scp Server Man-in-The-Middle Attack Vulnerability (127851) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
Apache HTTP Server 'mod_rewrite' Redirect Vulnerability (133604) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server URL Redirect Vulnerability (129591) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
OpenSSH Sensitive Data Exposure Vulnerability (146710) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH 'auth-gss2.c' User Detection Vulnerability (126832) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
Apache HTTP Server 'mod_http2' Read-After-Free (CVE-2019-0196) (128447) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'mod_session_cookie' Expiry Time Ignored Vulnerability (126276) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'mod_cache_socache' Out of Bound Read Denial of Service Vulnerability (126242) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		

Apache HTTP Server Slow Request Bodies Denial of Service Vulnerability (126273) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'httpd' URL Normalization Inconsistency Vulnerability (128448) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'Cache-Digest' Denial of Service Vulnerability (137995) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
OpenSSH User Enumeration Vulnerability (126863) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
Apache HTTP Server HTTP/2 Connections Crafted Request Denial of Service Vulnerability (908009) **internal | potential | unauth**	80 / tcp http	Medium
apache 2.4.29		
Apache HTTP Server 'mod_http2' Memory Corruption Vulnerability (129588) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server Crafted Request Denial of Service Vulnerability (127001) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
OpenSSH Privilege Escalation Vulnerability (146711) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH Account Enumeration Vulnerability (126640) **internal | potential | unauth**	22 / tcp ssh	Medium

7.6p1

OpenSSH 'Observable Discrepancy' Man-in-the-Middle Vulnerability (137503)
internal | potential | unauth
22 / tcp
ssh
Medium

7.6p1

Apache HTTP Server 'mod_proxy' Cross-Site Scripting Vulnerability (129590)
internal | potential | unauth
80 / tcp
http
Medium

2.4.29

Apache HTTP 'HTTP/2 mod' Denial of Service Vulnerability (137993)
internal | potential | unauth
80 / tcp
http
Medium

2.4.29

Apache HTTP Server 'SETTINGS' Denial of Service Vulnerability (126966)
internal | potential | unauth
80 / tcp
http
Medium

2.4.29

OpenSSH Missing Character Man-in-The-Middle Attack Vulnerability (127849)
internal | potential | unauth
22 / tcp
ssh
Medium

7.6p1

OpenSSH 'stderr' Man-in-The-Middle Attack Vulnerability (127850)
internal | potential | unauth
22 / tcp
ssh
Medium

7.6p1

OpenSSH Security Advisory (148395)
internal | potential | unauth
22 / tcp
ssh
Low

7.6p1

OpenSSH scp Client Access Bypass Vulnerability (127848)
internal | potential | unauth
22 / tcp
ssh
Low

7.6p1

Apache HTTP Server Denial of Service (902560) **internal | potential | unauth**	80 / tcp http	Trivial
2.4.29		

Content Security Policy Missing (148043) **internal | explicit | unauth**	80 / tcp http	Trivial
Missing Content Security Policy.		

WIN2019DC	**D**

IP: 10.27.34.88
Asset name: WIN2019DC
Operating system: Windows Server 2016
Asset type: Domain controller

Protocol	Service
kerberos-sec	88 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
ldap	389 / tcp
unknown	445 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Success	N/A	Success	Success

Authenticated Scan Credentials Used Successfully

OS: MyRNA Azure ACME
CIS: MyRNA Azure ACME
Threatscan: MyRNA Azure ACME

Vulnerability Title	Service(s)	Severity
MS22-JUN: Microsoft Windows Security Update (148994) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS22-JUN Vulnerable Path: C:\windows\system32\ntoskrnl.exe File Version: 10.0.14393.4770 Fixed Version: 10.0.14393.5192 Remediation KB(s): KB5014702		
MS22-APR: Microsoft Windows Security Update (148319) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS22-APR Vulnerable Path: C:\windows\system32\ntoskrnl.exe File Version: 10.0.14393.4770 Fixed Version: 10.0.14393.5066 Remediation KB(s): KB5012596		
MS22-MAY: Microsoft Windows Security Update (148572) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS22-MAY Vulnerable Path: C:\windows\system32\ntoskrnl.exe File Version: 10.0.14393.4770 Fixed Version: 10.0.14393.5125 Remediation KB(s): KB5013952		
MS21-DEC: Microsoft Windows Security Update (147272) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS21-DEC Vulnerable Path: C:\windows\system32\pcadm.dll File Version: 10.0.14393.4770 Fixed Version: 10.0.14393.4825 Remediation KB(s): KB5008207		
MS22-JAN: Microsoft Windows Security Update (147420) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS22-JAN Vulnerable Path: C:\windows\system32\pcadm.dll File Version: 10.0.14393.4770 Fixed Version: 10.0.14393.4886 Remediation KB(s): KB5009546		
MS22-MAR: Microsoft Windows Security Update (148037) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS22-MAR Vulnerable Path: C:\windows\system32\ntoskrnl.exe File Version: 10.0.14393.4770 Fixed Version: 10.0.14393.5006 Remediation KB(s): KB5011495		

MS22-MAR: Microsoft Internet Explorer Security Update (148036)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS22-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.14393.4770
Fixed Version: 11.0.14393.5006
Remediation KB(s): KB5011495

MS22-JUL: Microsoft Windows Security Update (149222)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS22-JUL
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 10.0.14393.4770
Fixed Version: 10.0.14393.5246
Remediation KB(s): KB5015808

MS22-FEB: Microsoft Windows Security Update (147753)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS22-FEB
Vulnerable Path: C:\windows\system32\pcadm.dll
File Version: 10.0.14393.4770
Fixed Version: 10.0.14393.4946
Remediation KB(s): KB5010359

MS20-NOV: Microsoft Windows Security Update - Registry Entry Not Set (143527)

N/A / tcp
unknown

High

internal | explicit | OS auth

Detected: Not set
Expected: 2

MS18-JAN: Microsoft Windows Security Update - Registry Entry Not Set (128655)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

MS18-JAN: Update is installed but the registry entry has not been set.

MS19-MAY: Microsoft Windows Security Update (ZombieLoad) - Registry Entry Not Set (128823)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

MS19-MAY: Update is installed but the registry entry has not been set.

LDAP Signing Vulnerability (129050)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

LDAP Signing is not required on this domain controller.

LDAP Channel Binding Vulnerability (132377)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

LDAP Channel Binding is not required on this domain controller.

MS18-NOV: Microsoft Windows Security Update - Registry Entry Not Set (128666) internal | explicit | OS auth	N/A / tcp unknown	Medium

MS18-NOV: Update is installed but the registry entry has not been set.

MS19-NOV: Microsoft Windows Security Update - Registry Entry Not Set (131738) internal | explicit | OS auth	N/A / tcp unknown	Medium

MS19-NOV: Update is installed but the registry entry has not been set.

Threat Scan: Windows Defender Definitions Outdated (126741) internal | explicit | Threat Scan auth	N/A / tcp unknown	Medium

Definitions last updated: 05/19/2016 21:28:52
Detected definition version: 1.221.14.0

SMB Null Session Authentication (101373) internal | recon | unauth	445 / tcp unknown	Trivial

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110) internal | explicit | unauth	3389 / tcp msrdp	Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.1:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) internal | explicit | unauth	3389 / tcp msrdp	Trivial

[Large data section omitted]

CIS Benchmark Profile (116437) internal | compliance | OS auth	N/A / tcp unknown	Trivial

CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0:DC2

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (122895) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (123252) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (122884) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Expected: >= 24
Collected: 0
Result: FAIL

SMB Native LanMan Version (100092) 445 / tcp Trivial

internal | **recon** | **unauth** unknown

LAN Manager: 10.0.14393.15
Domain: acme
OS: Windows 2016 Build 14393

Kerberos User Enumeration Detected (138135) 88 / tcp Trivial

internal | **explicit** | **unauth** kerberos-sec

Kerberos User Enum confirmed with krbtgt user on domain ACME

Compliance: Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (123133) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (122937) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Expected: Administrators,NT SERVICE\\WdiServiceHost
Collected: ADMINISTRATORS,NT SERVICE\WdiServiceHost
Result: PASS

Compliance: Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only) (122955) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (123210)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Select when Feature Updates are received' is set to 'Enabled: Current Branch for Business, 180 days' (123254)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (123003)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 1
Collected: 1
Result: PASS

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (123112)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: [Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1.*[Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off printing over HTTP' is set to 'Enabled' (123137)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Access this computer from the network' (122896)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,Authenticated Users,ENTERPRISE DOMAIN CONTROLLERS
Collected: EVERYONE,AUTHENTICATED USERS,ADMINISTRATORS,ALIAS PREW2KCOMPACC,ENTERPRISE DOMAIN CONTROLLERS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (123039) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Authorization Policy Change' is set to 'Success' (123068) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS Collected: AUDIT_NONE Result: FAIL		
Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123187) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (123245) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Prevent bypassing SmartScreen prompts for sites' is set to 'Enabled' (123207) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (123126) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 3 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (123145) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (122964)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (123036)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (123004)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Configure 'Allow log on locally' (122901)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS,ACCOUNT OPERATORS,SERVER OPERATORS,PRINTER OPERATORS,BACKUP OPERATORS,ENTERPRISE DOMAIN CONTROLLERS
Result: FAIL

Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (122905)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS,SERVER OPERATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (122890)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Join Microsoft MAPS' is set to 'Disabled' (123234) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (123196) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (123180) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (123241) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Process Creation' is set to 'Success' (123056) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS Collected: AUDIT_NONE Result: FAIL		
Compliance: Ensure 'Block launching Windows Store apps with Windows Runtime API access from hosted content.' is set to 'Enabled' (123171) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Do not allow COM port redirection' is set to 'Enabled' (123212) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (123091)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Remote Shell Access' is set to 'Disabled' (123253)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (123147)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (123104)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (123076)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (123159)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (122970)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: <= 14
Collected: 5
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log' (123024)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (122952)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only) (122930)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS,PERFLOG USERS
Result: PASS

Compliance: Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On' (123238)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (123086)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (122911)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Allow Extensions' is set to 'Disabled' (123198)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (123026)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Toggle user control over Insider builds' is set to 'Disabled' (123184)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require pin for pairing' is set to 'Enabled' (123178)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (123260)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (123142)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (123120)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (123232)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (123141)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (122908)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (123215)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (123138)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (123158) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (123237) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (123244) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security State Change' is set to 'Success' (123072) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (122923) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS,SERVER OPERATORS
Result: FAIL

Compliance: Ensure 'Configure Password Manager' is set to 'Disabled' (123201) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: no
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (123135) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (123030)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (122906)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS,SERVER OPERATORS
Result: FAIL

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (123179)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (122934)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (123115)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (123040)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (123011)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: 5
Result: FAIL

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (122910)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (122956)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Configure 'Accounts: Rename guest account' (122948)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: not Guest
Collected: Guest
Result: FAIL

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (123087)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (122962)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (122945) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (123109) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (123029) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (122939) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS,SERVER OPERATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (123114) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 255
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (122983) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (123124) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (123070)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (123095)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: <= 90
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (122958)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Group Membership' is set to 'Success' (123060)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (123033)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (123139)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (123216)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable Windows NTP Client' is set to 'Enabled' (123166)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Continue experiences on this device' is set to 'Disabled' (123129)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (123092)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Use of Camera' is set to 'Disabled' (123176)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (123063)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (123227)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (123041)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (123150)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (123019)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (122994)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: ^$
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (123156)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Untrusted Font Blocking' is set to 'Enabled: Block untrusted fonts and log events' (123154)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1000000000000
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (123148)

N/A / tcp

unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (122967)

N/A / tcp

unknown

Trivial

internal | compliance | CIS auth

Expected: [a-zA-Z]
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (123242)

N/A / tcp

unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (123074)

N/A / tcp

unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Allow InPrivate Browsing' is set to 'Disabled' (123199)

N/A / tcp

unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (123046)

N/A / tcp

unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (122959)

N/A / tcp

unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (123221)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 60000
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (122974)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Configure 'Network access: Remotely accessible registry paths and sub-paths' (122991)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

[Large data section omitted]

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123191)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (123172)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (123065)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (122927)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Configure 'Manage auditing and security log' (122931)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (123049)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (123084)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Deny access to this computer from the network' (122915)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (123155)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (123218)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (122996) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Watson events' is set to 'Disabled' (123236) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (123062) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (123053) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely ... (123085) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not show feedback notifications' is set to 'Enabled' (123183) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (123054) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (122949)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (123160)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

IPv6 Enabled (142306)

N/A / tcp
unknown

Trivial

internal | explicit | OS auth

IPv6 enabled on network interfaces with the following IPv4 addresses

10.27.34.88
10.27.34.88

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (123047)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (123015)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Debug programs' is set to 'Administrators' (122914)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (123023)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Network access: Remotely accessible registry paths' (122990)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: ^((System\\CurrentControlSet\\Control\\ProductOptions)|(System\\CurrentControlSet\\Control\\Server Applications)|(Software\\Microsoft\\Windows NT\\CurrentVersion))$
Collected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Result: PASS

Compliance: Configure 'Network access: Named Pipes that can be accessed anonymously' (122988)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: .+
Collected:
netlogon
samr
lsarpc
Result: FAIL

Compliance: Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only) (122954)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: 1
Result: FAIL

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (123152)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (123168)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (122920)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (123006)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log' (123034)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (123121)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (123190)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (122898)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (123017)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (122998)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (123240)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent access to the about:flags page in Microsoft Edge' is set to 'Enabled' (123205)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (123211)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (123250)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (123009)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (123153)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (122965)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: not 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Use enhanced anti-spoofing when available' is set to 'Enabled' (123175)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a service' to include 'Guests' (122918)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less' (123219)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 900000
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (123214)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (122977) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 15
Collected: 15
Result: PASS

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (122979) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure search suggestions in Address bar' is set to 'Disabled' (123203) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (123075) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create a token object' is set to 'No One' (122909) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (123012) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 3
Result: FAIL

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (122951)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Input Personalization' is set to 'Disabled' (123077)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow search and Cortana to use location' is set to 'Disabled' (123228)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (123134)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]' (123181)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off access to the Store' is set to 'Enabled' (123131)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled' (123193)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (123052)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (122968)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: [a-zA-Z]
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (123045)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (123048)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (123028)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable Font Providers' is set to 'Disabled' (123098)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (123090)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (123035)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (122924)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE
Result: PASS

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123189)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (123128)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (123247)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (123261) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (123093) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 3 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (123192) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: >= 32768 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (122963) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 0 Result: FAIL		
Compliance: Ensure 'Turn off the Store application' is set to 'Enabled' (123233) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (122999) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 2147483644 Collected: Not Defined Result: FAIL		

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (123018)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (123043)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (123013)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Synchronize directory service data' is set to 'No One' (DC only) (122941)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (123111)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (123089)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (122987)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (123151)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (122950)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (123066)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (123188)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 196608
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (123069)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (123094)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (123042) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (123257) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (123231) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (123249) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM&NTLM' (123002) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (122957) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (122997) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (122942)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) (122953)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (123209)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (123016)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Distribution Group Management' is set to 'Success and Failure' (DC only) (123051)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Turn off location' is set to 'Enabled' (123197)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (123021)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (122986)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (122894)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (122891)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (123163)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (123025)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Profile single process' is set to 'Administrators' (122936)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (122973)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: ^(1|2|3)$
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (123027)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (122992)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (122928)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,PRINTER OPERATORS
Result: FAIL

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (123194)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (122917)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Audit Account Lockout' is set to 'Success and Failure' (123059) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_SUCCESS Result: FAIL		
Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (123174) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 255 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (123222) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Directory Service Access' is set to 'Success and Failure' (DC only) (123057) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_SUCCESS Result: FAIL		
Compliance: Ensure 'Audit PNP Activity' is set to 'Success' (123055) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS Collected: AUDIT_NONE Result: FAIL		
Compliance: Ensure 'Add workstations to domain' is set to 'Administrators' (DC only) (122899) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: Administrators Collected: AUTHENTICATED USERS Result: FAIL		
Compliance: Ensure 'Deny log on locally' to include 'Guests' (122919) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (123223)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (123213)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Allow log on through Remote Desktop Services' (122903)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators,Remote Desktop Users
Collected: ADMINISTRATORS
Result: FAIL

Compliance: Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (123132)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disable pre-release features or settings' is set to 'Disabled' (123182)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (123186)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (123125)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Link Local Multicast Name Resolution (LLMNR) Enabled (129962)

N/A / tcp
unknown

Trivial

internal | **recon** | **OS auth**

LLMNR is enabled

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (123127)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable insecure guest logons' is set to 'Disabled' (123099)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disable all apps from Windows Store' is set to 'Enabled' (123230)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123185)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Enable computer and user accounts to be trusted for delegation' (122921)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: ADMINISTRATORS
Result: FAIL

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (122944) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (123010) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (123130) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: PASS

Compliance: Ensure 'Audit Special Logon' is set to 'Success' (123064) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (123217) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (123170) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Directory Service Changes' is set to 'Success and Failure' (DC only) (123058)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Configure 'Accounts: Rename administrator account' (122947)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: not Administrator
Collected: impact
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (123037)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (123001)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (123259)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (122887)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Turn off the advertising ID' is set to 'Enabled' (123165)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (122995) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (123195) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (122980) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (123157) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (122975) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (123005) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (123031)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party cookies' or higher (123200)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: <= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (123108)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (123071)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (122943)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (122889)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (122892)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: <= 10
Collected: 0
Result: PASS

Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (122981) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (123100) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (123229) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (122935) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Configure 'Impersonate a client after authentication' (122925) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Configure SmartScreen Filter' is set to 'Enabled' (123204) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (122907)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS,SERVER OPERATORS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (123032)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (123014)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (123246)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (123243)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (123173)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Cortana' is set to 'Disabled' (123225)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (123088)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 300000
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (122885)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 60
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (123177)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (123007)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (123022)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (123224)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (123164) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (123050) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (123067) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (123136) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (123248) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent using Localhost IP address for WebRTC' is set to 'Enabled' (123208) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Cortana above lock screen' is set to 'Disabled' (123226) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Modify an object label' is set to 'No One' (122933)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (123144)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Logoff' is set to 'Success' (123061)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (123038)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (122888)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 14
Collected: 4
Result: FAIL

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (123000)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (123073)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Configure Pop-up Blocker' is set to 'Enabled' (123202) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: yes
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (123140) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (122938) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE
Result: PASS

Compliance: Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (123143) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (123110) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (123020) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Lock pages in memory' is set to 'No One' (122929)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (123008)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Let Windows apps *' is set to 'Enabled: Force Deny' (123169)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (122960)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: > 0
Collected: 30
Result: PASS

Compliance: Ensure 'Shut down the system' is set to 'Administrators' (122940)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,SERVER OPERATORS,PRINTER OPERATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (123149)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (122976)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (122900)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Prevent bypassing SmartScreen prompts for files' is set to 'Enabled' (123206)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (123251)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Create symbolic links' (122912)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (122946)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log' (123044)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: %systemroot%\system32\logfiles\firewall\publicfw.log
Collected: Not Defined
Result: FAIL

TLS Connection: TLS Version 1.1 Enabled (145426)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

	Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641) internal | explicit | unauth	3389 / tcp msrdp	Trivial
	Server supports TLS version 1.0	

ADSERV-WIN16 D

IP: 192.168.0.109
Asset name: ADSERV-WIN16
Operating system: Windows Server 2016
Asset type: Domain controller

Protocol	Service
kerberos-sec	88 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
ldap	389 / tcp
smb	445 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Windows EFSRPC NTLM Relay Vulnerability (PetitPotam) (146093) internal | explicit | unauth	445 / tcp smb	High
[Large data section omitted]		

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | explicit | unauth

3389 / tcp
msrdp

Low

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - TLSv1
RC4-MD5 - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SMB Null Session Authentication (101373)

internal | recon | unauth

445 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

SMB Domain SID Disclosure (100872)

internal | explicit | unauth

445 / tcp
smb

Trivial

S-1-5-21-3985647337-4204166677-3319358195

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - TLSv1
RC4-MD5 - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

Kerberos User Enumeration Detected (138135) **internal** | **explicit** | **unauth**	88 / tcp kerberos-sec	Trivial
Kerberos User Enum confirmed with krbtgt user on domain ISMAILDOMAIN		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
Server supports TLS version 1.1		
SMB Native LanMan Version (100092) **internal** | **recon** | **unauth**	445 / tcp smb	Trivial
LAN Manager: Windows Server 2016 Datacenter 6.3 Domain: ISMAILDOMAIN OS: Windows Server 2016 Datacenter 14393		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
Server supports TLS version 1.0		

192.168.0.112 D

IP: 192.168.0.112
Asset name: 192.168.0.112
Operating system: VMware ESXi Server
Asset type: Server

Protocol	Service
unknown	80 / tcp
svrloc	427 / tcp
unknown (ssl)	443 / tcp
gsoap (ssl)	9080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity

VMware Security Advisory: VMSA-2019-0012 (129470)

N/A / tcp
unknown

High

internal | explicit | unauth

Missing VMware patches: ESXi670-201904101-SG
VMware Server Version: 6.7
Fixed Build: 13006603
Host Build: 8169922

VMware Security Advisory: VMSA-2020-0023 (142849)

N/A / tcp
unknown

High

internal | explicit | unauth

Missing VMware patches: ESXi670-202008101-SG
VMware Server Version: 6.7
Fixed Build: 16713306
Host Build: 8169922

VMware Security Advisory: VMSA-2021-0002 (144096)

N/A / tcp
unknown

High

internal | explicit | unauth

Missing VMware patches: ESXi670-202102401-SG
VMware Server Version: 6.7
Fixed Build: 17499825
Host Build: 8169922

VMware Security Advisory: VMSA-2018-0026 (126662)

N/A / tcp
unknown

High

internal | explicit | unauth

Missing VMware patches: ESXi670-201810101-SG
VMware Server Version: 6.7
Fixed Build: 10302608
Host Build: 8169922

VMware Security Advisory: VMSA-2020-0026 (143435)

N/A / tcp
unknown

High

internal | explicit | unauth

Missing VMware patches: ESXi670-202011101-SG
VMware Server Version: 6.7
Fixed Build: 17167734
Host Build: 8169922

VMware Security Advisory: VMSA-2019-0022 (131818)

N/A / tcp
unknown

High

internal | explicit | unauth

Missing VMware patches: ESXi670-201912001
VMware Server Version: 6.7
Fixed Build: 15160138
Host Build: 8169922

VMware Security Advisory: VMSA-2015-0007 (121637)

N/A / tcp
unknown

High

internal | explicit | unauth

Missing VMware patches: ESXi670-201806401-BG
VMware Server Version: 6.7
Fixed Build: 8941472
Host Build: 8169922

VMware Security Advisory: VMSA-2021-0014 (148212)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-202103101-SG
VMware Server Version: 6.7
Fixed Build: 17700523
Host Build: 8169922

VMware Security Advisory: VMSA-2020-0008 (137342)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-202004103-SG
VMware Server Version: 6.7
Fixed Build: 16075168
Host Build: 8169922

VMware Security Advisory: VMSA-2020-0012 (137344)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-202006401-SG
VMware Server Version: 6.7
Fixed Build: 16316930
Host Build: 8169922

VMware Security Advisory: VMSA-2020-0015 (137463)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-202006401-SG
VMware Server Version: 6.7
Fixed Build: 16075168
Host Build: 8169922

VMware Security Advisory: VMSA-2018-0016 (127203)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-201806401-BG
VMware Server Version: 6.7
Fixed Build: 8941472
Host Build: 8169922

VMware Security Advisory: VMSA-2022-0001 (148215)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-202111101-SG
VMware Server Version: 6.7
Fixed Build: 18828794
Host Build: 8169922

VMware Security Advisory: VMSA-2022-0004 (148216)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-202111101-SG
VMware Server Version: 6.7
Fixed Build: 18828794
Host Build: 8169922

VMware Security Advisory: VMSA-2019-0013 (129784)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-201810101-SG
VMware Server Version: 6.7
Fixed Build: 10302608
Host Build: 8169922

VMware Security Advisory: VMSA-2019-0006 (129035)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-201904101-SG
VMware Server Version: 6.7
Fixed Build: 13006603
Host Build: 8169922

VMware Security Advisory: VMSA-2018-0018 (126661)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-201806401-BG
VMware Server Version: 6.7
Fixed Build: 8941472
Host Build: 8169922

VMware Security Advisory: VMSA-2020-0018 (138134)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-202008101-SG, ESXi670-202008401-BG
VMware Server Version: 6.7
Fixed Build: 16713306
Host Build: 8169922

VMware Security Advisory: VMSA-2019-0020 (131817)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-201911402-BG
VMware Server Version: 6.7
Fixed Build: 15018017
Host Build: 8169922

VMware Security Advisory: VMSA-2018-0020 (126059)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-201808401-BG, ESXi670-201808402-BG, ESXi670-201808403-BG
VMware Server Version: 6.7
Fixed Build: 9484548
Host Build: 8169922

VMware Security Advisory: VMSA-2019-0008 (129335)

N/A / tcp
unknown

Medium

internal | explicit | unauth

Missing VMware patches: ESXi670-201905401-BG
VMware Server Version: 6.7
Fixed Build: 13644319
Host Build: 8169922

VMware Security Advisory: VMSA-2018-0012 (126058)

N/A / tcp

Medium

internal | explicit | unauth

unknown

Missing VMware patches: ESXi670-201806401-BG, ESXi670-201806402-BG
VMware Server Version: 6.7
Fixed Build: 8832884
Host Build: 8169922

VMware Security Advisory: VMSA-2018-0027 (127205)

N/A / tcp

Low

internal | explicit | unauth

unknown

Missing VMware patches: ESXi670-201811401-BG
VMware Server Version: 6.7
Fixed Build: 10764712
Host Build: 8169922

VMware Security Advisory: VMSA-2019-0014 (129785)

N/A / tcp

Low

internal | explicit | unauth

unknown

Missing VMware patches: ESXi670-201904101-SG
VMware Server Version: 6.7
Fixed Build: 13006603
Host Build: 8169922

VMware Security Advisory: VMSA-2019-0005 (128528)

N/A / tcp

Low

internal | explicit | unauth

unknown

Missing VMware patches: ESXi670-201903001
VMware Server Version: 6.7
Fixed Build: 13004448
Host Build: 8169922

VMware Security Advisory: VMSA-2022-0016 (149533)

N/A / tcp

Low

internal | explicit | unauth

unknown

Missing VMware patches: ESXi670-202206101-SG
VMware Server Version: 6.7
Fixed Build: 19898906
Host Build: 8169922

VMware Security Advisory: VMSA-2020-0011 (137343)

N/A / tcp

Low

internal | explicit | unauth

unknown

Missing VMware patches: ESXi670-202004101-SG
VMware Server Version: 6.7
Fixed Build: 15820472
Host Build: 8169922

VMware Security Advisory: VMSA-2019-0019 (131816)

N/A / tcp

Low

internal | explicit | unauth

unknown

Missing VMware patches: ESXi670-201908101-SG
VMware Server Version: 6.7
Fixed Build: 14320388
Host Build: 8169922

VMware Security Advisory: VMSA-2022-0020 (149535) internal | explicit | unauth	N/A / tcp unknown	Low
Missing VMware patches: ESXi670-202207401-SG VMware Server Version: 6.7 Fixed Build: 19997733 Host Build: 8169922		
Content Security Policy Missing (148043) internal | explicit | unauth	443 / tcp unknown (ssl)	Trivial
Missing Content Security Policy.		

HTORRES D

IP: 192.168.0.228
Asset name: HTORRES
Operating system: Windows 10 Enterprise
Asset type: Client

Protocol	Service
unknown	445 / tcp
vmwareauth	902 / tcp
vmwareauth	912 / tcp
general	N/A / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	Failure

Vulnerability Title	Service(s)	Severity
MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Registry Entry Not Set (149637) internal | explicit | OS auth	N/A / tcp general	High

MS13_098: Microsoft Security Update is installed but the registry entry has not been set.

Registry key incorrectly set:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck => None
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck => None

MS17-JUN: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128597)

N/A / tcp
general

Medium

internal | explicit | OS auth

MS17-JUN: Microsoft Internet Explorer Security Update is installed but the registry entry has not been set.

Registry keys missing:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1

MS17-SEP: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128598)

N/A / tcp
general

Medium

internal | explicit | OS auth

MS17-SEP: Microsoft Internet Explorer Security Update is installed but the registry entry has not been set.

Registry keys missing:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1

SMB Security Signatures Not Required (104188)

445 / tcp
unknown

Low

internal | explicit | unauth

SMBv2 NTLM signatures are not required

SMB Null Session Authentication (101373)

445 / tcp
unknown

Trivial

internal | recon | unauth

It was possible to log into the remote host using a NULL session.

SMB Native LanMan Version (100092)

445 / tcp
unknown

Trivial

internal | recon | unauth

LAN Manager: 10.0.19041.15
Domain: HTORRES0721
OS: Windows 10 Build 19041

Link Local Multicast Name Resolution (LLMNR) Enabled (129962)

N/A / tcp
general

Trivial

internal | recon | OS auth

LLMNR is enabled

NetBIOS Over TCP/IP Enabled (124295) internal | recon | OS auth	N/A / tcp general	Trivial

NetBIOS is enabled:
GUID: {634a4239-4e81-45f3-b9db-5bdaa4a6894e} - Value: 0
GUID: {70be01f5-0004-4fa8-b588-d4d2700ba51d} - Value: 0
GUID: {75e1ade8-74ae-4038-b245-19bb79429257} - Value: 0

IPv6 Enabled (142306) internal | explicit | OS auth	N/A / tcp general	Trivial

IPv6 enabled on network interfaces with the following IPv4 addresses
10.71.48.12
192.168.72.1
192.168.37.1

192.168.1.53 D

IP: 192.168.1.53
Asset name: 192.168.1.53
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Apache HTTP Server Security Update 2.4.48 (145498) internal | potential | unauth	80 / tcp http	High

2.4.29

Apache HTTP Server 'Module Scripts' Privilege Escalation Vulnerability (128443) internal | potential | unauth	80 / tcp http	High

2.4.29

Apache HTTP Server Internal Data Buffering Denial of Service Vulnerability (129589) **internal | potential | unauth**	80 / tcp http	High
2.4.29		
OpenSSH 'ssh-agent' Double Free Vulnerability (144213) **internal | potential | unauth**	22 / tcp ssh	High
7.6p1		
Apache HTTP Server 'mod_proxy_ftp' Uninitialized Memory Usage Vulnerability (133605) **internal | potential | unauth**	80 / tcp http	High
2.4.29		
Apache HTTP Server Multiple Vulnerabilities (126218) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'mod_http2' Read-After-Free (CVE-2019-10082) (129592) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
OpenSSH 'scp' Command Evaluation Vulnerability (138013) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
Apache HTTP Server 'mod_auth_digest' Access Control Bypass Vulnerability (128444) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'mod_session_cookie' Expiry Time Ignored Vulnerability (126276) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'mod_http2' Memory Corruption Vulnerability (129588) **internal | potential | unauth**	80 / tcp http	Medium

2.4.29		
Apache HTTP Server 'mod_cache_socache' Out of Bound Read Denial of Service Vulnerability (126242) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP 'HTTP/2 mod' Denial of Service Vulnerability (137993) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server Crafted Request Denial of Service Vulnerability (127001) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server HTTP/2 Connections Crafted Request Denial of Service Vulnerability (908009) **internal | potential | unauth**	80 / tcp http	Medium
apache 2.4.29		
Apache HTTP Server 'Cache-Digest' Denial of Service Vulnerability (137995) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
OpenSSH Missing Character Man-in-The-Middle Attack Vulnerability (127849) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH 'stderr' Man-in-The-Middle Attack Vulnerability (127850) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
Apache HTTP Server 'mod_rewrite' Redirect Vulnerability (133604) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		

Apache HTTP Server URL Redirect Vulnerability (129591) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'mod_proxy' Cross-Site Scripting Vulnerability (129590) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
OpenSSH 'Observable Discrepancy' Man-in-the-Middle Vulnerability (137503) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH scp Server Man-in-The-Middle Attack Vulnerability (127851) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
Apache HTTP Server 'SETTINGS' Denial of Service Vulnerability (126966) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'httpd' URL Normalization Inconsistency Vulnerability (128448) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
Apache HTTP Server 'mod_http2' Read-After-Free (CVE-2019-0196) (128447) **internal | potential | unauth**	80 / tcp http	Medium
2.4.29		
OpenSSH 'auth-gss2.c' User Detection Vulnerability (126832) **internal | potential | unauth**	22 / tcp ssh	Medium
7.6p1		
OpenSSH User Enumeration Vulnerability (126863) **internal | potential | unauth**	22 / tcp ssh	Medium

7.6p1		
Apache HTTP Server Slow Request Bodies Denial of Service Vulnerability (126273) internal | potential | unauth	80 / tcp http	Medium
2.4.29		
OpenSSH Account Enumeration Vulnerability (126640) internal | potential | unauth	22 / tcp ssh	Medium
7.6p1		
OpenSSH scp Client Access Bypass Vulnerability (127848) internal | potential | unauth	22 / tcp ssh	Low
7.6p1		
Apache HTTP Server Denial of Service (902560) internal | potential | unauth	80 / tcp http	Trivial
2.4.29		

LAPTOP-SU09C2DM	**D**

IP: 192.168.1.252
Asset name: LAPTOP-SU09C2DM
Operating system: Windows 11 Home
Asset type: Client

Protocol	Service
general	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Registry Entry Not Set (149637) internal | explicit | OS auth	N/A / tcp general	High

MS13_098: Microsoft Security Update is installed but the registry entry has not been set.

Registry key incorrectly set:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck => None
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Cryptography\Wintrust\Config\EnableCertPaddingCheck => None

MS17-JUN: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128597)

internal | explicit | OS auth

N/A / tcp
general

Medium

MS17-JUN: Microsoft Internet Explorer Security Update is installed but the registry entry has not been set.

Registry keys missing:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1

MS17-SEP: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128598)

internal | explicit | OS auth

N/A / tcp
general

Medium

MS17-SEP: Microsoft Internet Explorer Security Update is installed but the registry entry has not been set.

Registry keys missing:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1

Link Local Multicast Name Resolution (LLMNR) Enabled (129962)

internal | recon | OS auth

N/A / tcp
general

Trivial

LLMNR is enabled

NetBIOS Over TCP/IP Enabled (124295)

internal | recon | OS auth

N/A / tcp
general

Trivial

NetBIOS is enabled:
GUID: {9235256b-1a5b-45eb-ac83-ee6f15cbf99e} - Value: 0

IPv6 Enabled (142306)

internal | explicit | OS auth

N/A / tcp
general

Trivial

IPv6 is Enabled

S1-WIN2019-DC01 D

IP: 192.168.67.35
Asset name: S1-WIN2019-DC01
Operating system: Windows Server 2019
Asset type: Domain controller

Protocol	Service
kerberos-sec	88 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
ldap	389 / tcp
unknown	445 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Windows EFSRPC NTLM Relay Vulnerability (PetitPotam) (146093) **internal** | **explicit** | **unauth**	445 / tcp unknown	High
[Large data section omitted]		
SMB Null Session Authentication (101373) **internal** | **recon** | **unauth**	445 / tcp unknown	Trivial
It was possible to log into the remote host using a NULL session.		
SMB Native LanMan Version (100092) **internal** | **recon** | **unauth**	445 / tcp unknown	Trivial
LAN Manager: 10.0.17763.15 Domain: AD01 OS: Windows 2019 Build 17763		
Kerberos User Enumeration Detected (138135) **internal** | **explicit** | **unauth**	88 / tcp kerberos-sec	Trivial
Kerberos User Enum confirmed with krbtgt user on domain AD01		

WIN-30QQRC10MGG D

IP: 192.168.67.53
Asset name: WIN-30QQRC10MGG
Operating system: Windows Server 2012 R2
Asset type: Server

Protocol	Service
http	80 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
smb	445 / tcp
lpd	515 / tcp
winrm	5985 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) (117590) internal | explicit | unauth	80 / tcp http	High
[Large data section omitted]		
SMB Security Signatures Not Required (104188) internal | explicit | unauth	139 / tcp netbios	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (120674) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (120635)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (120658)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120809)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (120773)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create a token object' is set to 'No One' (120533)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (120704)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (120641) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Configure 'Accounts: Rename administrator account' (120563) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: not Administrator Collected: Administrator Result: FAIL		
Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (120544) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: Administrators Collected: ADMINISTRATORS Result: PASS		
Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (120652) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (120565) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (120712) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Configure 'Manage auditing and security log' (120548) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit Security State Change' is set to 'Success' (120678)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (120618)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (120717)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (120620)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: 0
Result: FAIL

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (120787)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (120628)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (120684)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (120608)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 2147483644
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (120640)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (120675)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (120688)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 30
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (120520)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (120568) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (120616) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (120607) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (120713) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (120751) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (120754) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (120647) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (120687) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120825) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges
Result: PASS

Compliance: Ensure 'Debug programs' is set to 'Administrators' (120537) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (120756) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings
Result: FAIL

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (120735) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a service' to include 'Guests' (120539) N/A / tcp Trivial

internal | **compliance** | **CIS auth** unknown

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (120663)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120767)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (120545)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (120592)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (120822)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments
Result: PASS

Compliance: Ensure 'Network access: Remotely accessible registry paths and sub-paths' (120601)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

[Large data section omitted]

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (120696)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (120657) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Password protect the screen saver' is set to 'Enabled' (120818) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Password protect the screen saver
Result: PASS

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (120585) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Audit Special Logon' is set to 'Success' (120671) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (120578) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (120650) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (120642) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (120518)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (120753)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (120597)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewalldomainfw.log' (120633)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (120553)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,NT SERVICE\\WdiServiceHost
Collected: ADMINISTRATORS,NT SERVICE\WdiServiceHost
Result: PASS

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (120610)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Configure 'Create symbolic links' (120536)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (120589)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (120676)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths' (120600)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Collected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Result: PASS

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (120659)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (120798)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (120794)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (120572) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (120737) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (120705) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable screen saver' is set to 'Enabled' (120816) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver
Result: PASS

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (120579) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (120624) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'EMET 5.5' or higher is installed (120755) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (120587) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (120595) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (120815) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (120519) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: >= 14
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120644) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120634) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (120686) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 4 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (120784) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 3 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (120742) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (120749) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (120530) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: Administrators,LOCAL SERVICE Collected: LOCAL SERVICE,ADMINISTRATORS Result: PASS		
Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (120750) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120543) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (120716)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (120689)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (120677)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (120760)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disa... (120691)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (120680)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (120623)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (120774)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (120805)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (120567)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (120617)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (120523)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
Result: FAIL

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (120779)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (120682)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (120528)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
Result: FAIL

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (120790)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (120817)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Force specific screen saver: Screen saver executable name
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (120638)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (120535)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (120639)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (120706)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
Result: FAIL

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (120772)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (120637)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120806)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (120761)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (120679)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (120631)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (120814)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120554)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (120629)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (120625)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (120559)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (120672)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120769)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (120521)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (120819)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Control Panel\Personalization\Screen saver timeout: Seconds
Result: PASS

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (120776)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (120551)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (120524)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (120582)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (120820)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallprivatefw.log' (120643)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (120651)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (120736)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (120655)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (120783) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Modify an object label' is set to 'No One' (120549) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (120577) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (120612) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: 1
Result: PASS

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (120599) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (120656) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (120605) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (120611)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (120813)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (120670)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Audit Logoff' is set to 'Success' (120668)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120810)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallpublicfw.log' (120653)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: %systemroot%\system32\logfiles\firewall\publicfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120801)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120768)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (120762)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (120609)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (120685)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (120700)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 90
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (120580)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (120636)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (120615)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (120743)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (120532)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (120529)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120763)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Protections for Popular Software' is set to 'Enabled' (120758)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Popular Software
Result: FAIL

Compliance: Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (120757)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: *\Internet Explorer\iexplore.exe
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (120752)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 255
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (120741)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (120621)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 3
Result: FAIL

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (120534)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (120649)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent the usage of SkyDrive for file storage' is set to 'Enabled' (120792)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (120803)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (120586)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1 or 2 or 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Audit Account Lockout' is set to 'Success' (120667)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (120808)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120770)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (120576)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age
Result: FAIL

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (120811)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (120710)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120614)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (120734)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Lock pages in memory' is set to 'No One' (120546)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (120590)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session
Result: FAIL

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (120718)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: PASS

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (120542)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (120526)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (120573)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (120738)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120764)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (120562) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (120581) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (120673) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120807) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (120550) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (120603) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: No Defined Values
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (120694)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (120516)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 24
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (120646)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (120795)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (120648)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (120683)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: C:\Program Files\LAPS\CSE\AdmPwd.dll
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (120800)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (120799)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (120560)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120613)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Profile single process' is set to 'Administrators' (120552)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120654)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' (120771)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (120566)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (120766)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 196608
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely... (120690)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (120692)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (120715)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (120525)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (120804) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (120538) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: Guests Collected: Empty string Result: FAIL		
Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (120697) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: <= 5 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Deny log on locally' to include 'Guests' (120540) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: Guests Collected: Empty string Result: FAIL		
Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (120602) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (120561) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 0 Collected: 1 Result: FAIL		
Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (120575) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (120662)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (120632)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (120574)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (120531)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (120555)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (120594)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (120645)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (120714)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (120604)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (120517)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
Result: FAIL

Compliance: Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (120823)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments
Result: PASS

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (120788)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (120593)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (120824)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile.
Result: PASS

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (120669)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (120584)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration
Result: PASS

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (120588)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (120541)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (120626)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (120627) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (120630) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (120661) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_NONE Result: FAIL		
Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (120789) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (120596) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (120606) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120765) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (120622)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (120558)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit Process Creation' is set to 'Success' (120664)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (120591)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (120782)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (120759)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software
Result: FAIL

Compliance: Ensure 'Shut down the system' is set to 'Administrators' (120556)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Configure 'Accounts: Rename guest account' (120564)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: not Guest
Collected: Guest
Result: FAIL

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (120522)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (120681)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (120619)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Default IIS Webpage Detected (117366)

80 / tcp
http

Trivial

internal | recon | unauth

Default IIS Webpage Detected

NTLM Authentication Host Information Disclosure (117943)

80 / tcp
http

Trivial

internal | recon | unauth

NetBIOS Domain: WIN-30QQRC10MGG
NetBIOS Hostname: WIN-30QQRC10MGG
DNS Domain Name: WIN-30QQRC10MGG
DNS Hostname: WIN-30QQRC10MGG

SMB Native LanMan Version (100092) internal | recon | unauth	139 / tcp netbios	Trivial

LAN Manager: 6.3.9600.15
Domain: WIN-30QQRC10MGG
OS: Windows 2012 R2 Build 9600

192.168.67.175 D

IP: 192.168.67.175
Asset name: 192.168.67.175
Operating system: Windows 7
Asset type: Client

Protocol	Service
ssh	22 / tcp
unknown	139 / tcp
vnc	5900 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Microsoft Windows 7 End of Life (131864) internal | explicit | unauth	N/A / tcp unknown	High
Support has ended for Windows 7. This host should be immediately upgraded.		
SMB Native LanMan Version (100092) internal | recon | unauth	139 / tcp unknown	Trivial
LAN Manager: 6.1.7600.0 Domain: MBP-MAC OS: Windows 7 Build 7600		

S1-WIN2012-WKGP D

IP: 192.168.67.242
Asset name: S1-WIN2012-WKGP
Operating system: Windows Server 2012 R2

Asset type: Server

Protocol	Service
http	80 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
lpd	515 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) (117590) **internal | explicit | unauth**	80 / tcp http	High
[Large data section omitted]		
MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756) **internal | explicit | unauth**	135 / tcp msrpc	Medium
This asset permits binding to samr pipe using auth level Connect. Response from asset: 02 . 22 00 00 c0 "... Responding port: 49158		

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | explicit | unauth

3389 / tcp
msrdp

Low

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SMB Security Signatures Not Required (104188)

internal | explicit | unauth

139 / tcp
netbios

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

Remote Desktop Protocol Allows Man in the Middle (117858)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: ECDHE-RSA-AES256-SHA

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

SMB Native LanMan Version (100092)

internal | recon | unauth

139 / tcp
netbios

Trivial

LAN Manager: 6.3.9600.15
Domain: S1-WIN2012-WKGP
OS: Windows 2012 R2 Build 9600

Default IIS Webpage Detected (117366)

internal | recon | unauth

80 / tcp
http

Trivial

Default IIS Webpage Detected

NTLM Authentication Host Information Disclosure (117943)

internal | recon | unauth

80 / tcp
http

Trivial

NetBIOS Domain: S1-WIN2012-WKGP
NetBIOS Hostname: S1-WIN2012-WKGP
DNS Domain Name: S1-Win2012-WKGP
DNS Hostname: S1-Win2012-WKGP

192.168.68.54 D

IP: 192.168.68.54
Asset name: 192.168.68.54
Operating system: Windows Platform
Asset type: Server

Protocol	Service
http	80 / tcp
netbios-ns	137 / udp

netbios	139 / tcp
smb	445 / tcp
winrm	5985 / tcp
http	8530 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Success	N/A	Success	N/A

Authenticated Scan Credentials Used Successfully

OS: Threat Domain
CIS: Threat Domain

Vulnerability Title	Service(s)	Severity
MS20-JUL: Microsoft Windows Security Update (137512) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS20-JUL Vulnerable Path: C:\windows\system32\windowscodecs.dll File Version: 6.3.9600.17415 Fixed Version: 6.3.9600.19749 Remediation KB(s): KB4565540,KB4565541,KB4566425		
MS19-FEB: Microsoft Windows Security Update (127998) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS19-FEB Vulnerable Path: C:\windows\system32\jscript.dll File Version: 5.8.9600.17416 Fixed Version: 5.8.9600.19267 Remediation KB(s): KB3173424,KB4487028,KB4487000		
MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) (117590) **internal | explicit | unauth**	80 / tcp http	High
[Large data section omitted]		
MS19-OCT: Microsoft Windows Security Update (129806) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS19-OCT
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19507
Remediation KB(s): KB4512938,KB4519990,KB4520005

MS20-MAY: Microsoft Windows Security Update (134000)
internal | **explicit** | **OS auth**
N/A / tcp
unknown
High

Missing Microsoft Patch: MS20-MAY
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19697
Remediation KB(s): KB4556853,KB4556846

MS21-JUL: Microsoft Windows Security Update (145614)
internal | **explicit** | **OS auth**
N/A / tcp
unknown
High

Missing Microsoft Patch: MS21-JUL
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20069
Remediation KB(s): KB5004958,KB5004233,KB5004298,KB5004954,KB5004285

MS19-NOV: Microsoft Windows Security Update (131731)
internal | **explicit** | **OS auth**
N/A / tcp
unknown
High

Missing Microsoft Patch: MS19-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19538
Remediation KB(s): KB4525243,KB4525250,KB4524445

MS21-MAY: Microsoft Windows Security Update (144994)
internal | **explicit** | **OS auth**
N/A / tcp
unknown
High

Missing Microsoft Patch: MS21-MAY
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20017
Remediation KB(s): KB5003220,KB5003209

MS20-DEC: Microsoft Windows Security Update (143512)
internal | **explicit** | **OS auth**
N/A / tcp
unknown
High

Missing Microsoft Patch: MS20-DEC
Vulnerable Path: C:\windows\system32\localspl.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19893
Remediation KB(s): KB4592495,KB4592484

MS17-JUN: Microsoft Windows Security Update (122281)
internal | **explicit** | **OS auth**
N/A / tcp
unknown
High

Missing Microsoft Patch: MS17-JUN
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18696
Remediation KB(s): KB4022726,KB4022717

MS21-AUG: Microsoft Windows Security Update (146090) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS21-AUG
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20094
Remediation KB(s): KB5005076,KB5005106

MS19-APR: Microsoft Windows Security Update (128576) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS19-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19328
Remediation KB(s): KB4493467,KB3173424,KB4493446

MS20-MAR: Microsoft Windows Security Update (132715) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS20-MAR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19650
Remediation KB(s): KB4541505,KB4541509

MS19-JAN: Microsoft Windows Security Update (127739) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS19-JAN
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19236
Remediation KB(s): KB3173424,KB4480963,KB4480964

MS20-JAN: Microsoft Windows Security Update (132230) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS20-JAN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19593
Remediation KB(s): KB4534297,KB4534309

MS19-MAR: Microsoft Windows Security Update (128290) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS19-MAR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19304
Remediation KB(s): KB4489883,KB3173424,KB4489881

MS22-MAY: Microsoft Windows Security Update (148572) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS22-MAY
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20369
Remediation KB(s): KB5014001,KB5014011

MS19-AUG: Microsoft Windows Security Update (129476) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS19-AUG
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19427
Remediation KB(s): KB4512489,KB4512488

MS17-JUL: Microsoft Windows Security Update (122296) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS17-JUL
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18737
Remediation KB(s): KB4025333,KB4025336

MS18-DEC: Microsoft Windows Security Update (127241) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS18-DEC
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19208
Remediation KB(s): KB3173424,KB4471322,KB4471320

MS22-APR: Microsoft Windows Security Update (148319) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS22-APR
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20334
Remediation KB(s): KB5012639,KB5012670

MS18-OCT: Microsoft Windows Security Update (126602) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS18-OCT
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19153
Remediation KB(s): KB4462926,KB4462941

MS22-JAN: Microsoft Windows Security Update (147420) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS22-JAN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20239
Remediation KB(s): KB5009595,KB5009624

MS20-APR: Microsoft Windows Security Update (133731) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS20-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19670
Remediation KB(s): KB4550961,KB4550970

MS21-JUN: Microsoft Windows Security Update (145281) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS21-JUN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20036
Remediation KB(s): KB5003636,KB5003681,KB5003671

MS17-DEC: Microsoft Windows Security Update (123544) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS17-DEC
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18872
Remediation KB(s): KB4054519,KB4054522

MS20-OCT: Microsoft Windows Security Update (142682) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS20-OCT
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19846
Remediation KB(s): KB4580347,KB4580358

MS21-APR: Microsoft Windows Security Update (144750) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS21-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19990
Remediation KB(s): KB5001393,KB5001382

MS17-SEP: Microsoft Windows Security Update (122555) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS17-SEP
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18790
Remediation KB(s): KB4038792,KB4038793

MS21-MAR: Microsoft Windows Security Update (144194) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-MAR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19968
Remediation KB(s): KB5000848,KB5000853

MS18-JUL: Microsoft Windows Security Update (125654) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-JUL
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19064
Remediation KB(s): KB4338815,KB4338824

MS20-NOV: Microsoft Windows Security Update (143189) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19867
Remediation KB(s): KB4586845,KB4586823

MS21-FEB: Microsoft Windows Security Update (144007) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-FEB
Vulnerable Path: C:\windows\system32\localspl.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19941
Remediation KB(s): KB4601384,KB4601349

MS21-DEC: Microsoft Windows Security Update (147272) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-DEC
Vulnerable Path: C:\windows\system32\spoolsv.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20201
Remediation KB(s): KB5008285,KB5008263

MS17-OCT: Microsoft Windows Security Update (122638)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-OCT
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18818
Remediation KB(s): KB4041687,KB4041693

MS19-SEP: Microsoft Windows Security Update (129633)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-SEP
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19457
Remediation KB(s): KB4516067,KB4516064,KB4512938

MS21-SEP: Microsoft Windows Security Update (146370)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-SEP
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20117
Remediation KB(s): KB5005613,KB5005627

MS19-MAY: Microsoft Windows Security Update (ZombieLoad) (128795)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-MAY
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19355
Remediation KB(s): KB4499165,KB3173424,KB4499151

MS21-JAN: Microsoft Windows Security Update (143778)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-JAN
Vulnerable Path: C:\windows\system32\localspl.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19920
Remediation KB(s): KB4598285,KB4598275

MS18-NOV: Microsoft Windows Security Update (126949)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19176
Remediation KB(s): KB3173424,KB4467703,KB4467697

MS22-JUN: Microsoft Windows Security Update (148994)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-JUN
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20396
Remediation KB(s): KB5014738,KB5014746

MS19-JUL: Microsoft Windows Security Update (129103)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-JUL
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19402
Remediation KB(s): KB4507448,KB4507457,KB4504418

MS21-NOV: Microsoft Windows Security Update (146938)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20165
Remediation KB(s): KB5007255,KB5007247

MS15-043: Cumulative Security Update for Internet Explorer (117738)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS15-043
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17801

MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (118096)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS15-078
Vulnerable Path: C:\windows\system32\atmfd.dll
File Version: 5.1.2.238
Fixed Version: 5.1.2.243

MS15-018: Cumulative Security Update for Internet Explorer (117479)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS15-018
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17690

MS15-056: Cumulative Security Update for Internet Explorer (117878)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-056
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17842

MS15-009: Security Update for Internet Explorer (117381)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-009
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17631

MS15-032: Cumulative Security Update for Internet Explorer (117588)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-032
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17728

MS15-065: Security Update for Internet Explorer (118050)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-065
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17905

MS17-010: Security Update for Microsoft Windows SMB Server (121906)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: ms17-010
Vulnerable Path: C:\windows\system32\drivers\srv.sys
File Version: 6.3.9600.17238
Fixed Version: 6.3.9600.18604

MS15-021: Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (117476)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-021
Vulnerable Path: C:\windows\system32\atmfd.dll
File Version: 5.1.2.238
Fixed Version: 5.1.2.241

MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (118133)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-080
Vulnerable Path: C:\windows\system32\atmfd.dll
File Version: 5.1.2.238
Fixed Version: 5.1.2.245

MS15-079: Cumulative Security Update for Internet Explorer (118134)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-079
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17937

MS15-106: Cumulative Security Update for Internet Explorer (118394)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-106
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18052

MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (117737)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-044
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17796

MS15-093: Security Update for Internet Explorer (118245)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-093
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17963

MS15-124: Cumulative Security Update for Internet Explorer (118670)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS15-124
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18125

MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (116972)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS14-068
Vulnerable Path: C:\windows\system32\kerberos.dll
File Version: 6.3.9600.17340
Fixed Version: 6.3.9600.17423

MS21-JUL: Microsoft Windows Out-of-Band Security Update (145515)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-JUL
Vulnerable Path: C:\windows\system32\spoolsv.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20046
Remediation KB(s): KB5004954,KB5004958

MS16-146: Security Update for Microsoft Graphics Component (121325)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-146
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS16-147: Security Update for Microsoft Uniscribe (121324)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-147
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS20-SEP: Microsoft Internet Explorer Security Update (138218)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-SEP
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19811
Remediation KB(s): KB4577010,KB4577066

MS16-063: Cumulative Security Update for Internet Explorer (119505)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-063
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18349

MS16-040: Security Update for Microsoft XML Core Services (119275) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS16-040
Vulnerable Path: C:\windows\system32\msxml3.dll
File Version: 8.110.9600.17415
Fixed Version: 8.110.9600.18258

MS16-132: Security Update for Microsoft Graphics Component (121130) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS16-132
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18524

MS18-JUN: Microsoft Windows Security Update (125544) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-JUN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19000
Remediation KB(s): KB4284878,KB4284815

MS16-009: Cumulative Security Update for Internet Explorer (118985) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS16-009
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18205

MS18-APR: Microsoft Internet Explorer Security Update (123954) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-APR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18978
Remediation KB(s): KB4093114,KB4092946

MS20-FEB: Microsoft Windows Security Update (132516) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-FEB
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19630
Remediation KB(s): KB4537821,KB4502496,KB4537803

MS21-AUG: Microsoft Internet Explorer Security Update (146092)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-AUG
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19404
Remediation KB(s): KB5005036

MS20-SEP: Microsoft Windows Security Update (138219)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-SEP
Vulnerable Path: C:\windows\system32\puiobj.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19810
Remediation KB(s): KB4577066,KB4577071

MS20-JUN: Microsoft Windows Security Update (137200)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-JUN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19727
Remediation KB(s): KB4561666,KB4561673

MS22-JUL: Microsoft Windows Security Update (149222)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-JUL
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20475
Remediation KB(s): KB5015874,KB5015877

MS18-APR: Microsoft Windows Security Update (123955)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18979
Remediation KB(s): KB4093115,KB4093114

MS16-144: Cumulative Security Update for Internet Explorer (121327)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-144
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS22-MAR: Microsoft Windows Security Update (148037) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS22-MAR
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20302
Remediation KB(s): KB5011564,KB5011560

MS16-104: Cumulative Security Update for Internet Explorer (120918) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS16-104
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18450

MS20-AUG: Microsoft Windows Security Update (138007) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS20-AUG
Vulnerable Path: C:\windows\system32\puiobj.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19785
Remediation KB(s): KB4571723,KB4571703

MS18-MAY: Microsoft Internet Explorer Security Update (124365) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS18-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19003
Remediation KB(s): KB4103768,KB4103725

MS19-MAY: Microsoft Internet Explorer Security Update (128794) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS19-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19355
Remediation KB(s): KB4499151,KB4498206

MS18-AUG: Microsoft Windows Security Update (125932) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS18-AUG
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19095
Remediation KB(s): KB4343898,KB4343888

MS17-AUG: Microsoft Windows Security Update (122397)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-AUG
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18759
Remediation KB(s): KB4034672,KB4034681

MS22-FEB: Microsoft Windows Security Update (147753)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-FEB
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20269
Remediation KB(s): KB5010395,KB5010419

MS19-DEC: Microsoft Windows Security Update (131867)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-DEC
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19574
Remediation KB(s): KB4530730,KB4530702,KB4524445

MS18-SEP: Microsoft Windows Security Update (126401)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-SEP
Vulnerable Path: C:\windows\system32\windowscodecs.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19133
Remediation KB(s): KB4457143,KB4457129

MS20-APR: Microsoft Internet Explorer Security Update (133730)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-APR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19671
Remediation KB(s): KB4550905,KB4550961

MS19-JUN: Microsoft Windows Security Update (128962)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-JUN
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19377
Remediation KB(s): KB3173424,KB4503276,KB4503290

MS18-MAY: Microsoft Windows Security Update (124366)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-MAY
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19000
Remediation KB(s): KB4103715,KB4103725

MS18-AUG: Microsoft Internet Explorer Security Update (125931)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-AUG
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19101
Remediation KB(s): KB4343205,KB4343898

MS20-NOV: Microsoft Internet Explorer Security Update (143188)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-NOV
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19867
Remediation KB(s): KB4586768,KB4586845

MS17-APR: Microsoft Windows Security Update (122045)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18623
Remediation KB(s): KB4015550

MS17-MAY: Microsoft Windows Security Update (122154)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-MAY
Vulnerable Path: C:\windows\system32\urlmon.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18666
Remediation KB(s): KB4019215

MS16-087: Security Update for Windows Print Spooler Components (119630)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-087
Vulnerable Path: C:\windows\system32\win32spl.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18398

MS17-013: Security Update for Microsoft Graphics Component (121903) N/A / tcp unknown High
internal | explicit | OS auth

Missing Microsoft Patch: MS17-013
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18603

MS18-FEB: Microsoft Windows Security Update (123788) N/A / tcp unknown High
internal | explicit | OS auth

Missing Microsoft Patch: MS18-FEB
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18907
Remediation KB(s): KB4074597,KB4074594

MS21-SEP: Microsoft Internet Explorer Security Update (146369) N/A / tcp unknown High
internal | explicit | OS auth

Missing Microsoft Patch: MS21-SEP
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19404
Remediation KB(s): KB5005563,KB5005613,KB5005627

MS16-039: Security Update for Microsoft Graphics Component (119276) N/A / tcp unknown High
internal | explicit | OS auth

Missing Microsoft Patch: MS16-039
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18290

MS16-028: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (119089) N/A / tcp unknown High
internal | explicit | OS auth

Missing Microsoft Patch: MS16-028
Vulnerable Path: C:\windows\system32\glcndfilter.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18229

MS18-MAR: Microsoft Windows Security Update (123856) N/A / tcp unknown High
internal | explicit | OS auth

Missing Microsoft Patch: MS18-MAR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18954
Remediation KB(s): KB4088879,KB4088876

MS16-012: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (118984)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-012
Vulnerable Path: C:\windows\system32\glcndfilter.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18184

MS16-130: Security Update for Microsoft Windows (121132)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-130
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18524

MS16-037: Cumulative Security Update for Internet Explorer (119278)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-037
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18281

MS17-DEC: Microsoft Internet Explorer Security Update (123543)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-DEC
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18860
Remediation KB(s): KB4052978,KB4054519

MS19-DEC: Microsoft Internet Explorer Security Update (131866)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-DEC
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19572
Remediation KB(s): KB4530677,KB4530702

MS20-JUL: Microsoft Internet Explorer Security Update (137511)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-JUL
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19750
Remediation KB(s): KB4565479,KB4565541

MS20-JUN: Microsoft Internet Explorer Security Update (137199)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-JUN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19724
Remediation KB(s): KB4561603,KB4561666

MS17-NOV: Microsoft Internet Explorer Security Update (122791)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-NOV
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18817
Remediation KB(s): KB4047206,KB4048958

MS19-JUN: Microsoft Internet Explorer Security Update (128961)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-JUN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19377
Remediation KB(s): KB4503259,KB4503276,KB4503290

MS18-MAR: Microsoft Internet Explorer Security Update (123855)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18953
Remediation KB(s): KB4088876,KB4089187

MS21-MAR: Microsoft Internet Explorer Security Update (144193)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19963
Remediation KB(s): KB5000848,KB5000800

MS17-006: Cumulative Security Update for Internet Explorer (121910)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-006
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18618

MS19-MAR: Microsoft Internet Explorer Security Update (128289)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19301
Remediation KB(s): KB4489881,KB4489873

MS17-APR: Microsoft Internet Explorer Security Update (122044)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-APR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18639
Remediation KB(s): KB4014661,KB4015550

MS18-FEB: Microsoft Internet Explorer Security Update (123787)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-FEB
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18921
Remediation KB(s): KB4074594,KB4074736

MS18-JUL: Microsoft Internet Explorer Security Update (125653)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-JUL
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19061
Remediation KB(s): KB4338815,KB4339093

MS16-116: Security Update in OLE Automation for VBScript Scripting Engine (120906)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-116
Vulnerable Path: C:\windows\system32\oleaut32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18434

MS17-JUL: Microsoft Internet Explorer Security Update (122295)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-JUL
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18739
Remediation KB(s): KB4025252,KB4025336

MS16-023: Cumulative Security Update for Internet Explorer (119094)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-023
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18231

MS19-JUL: Microsoft Internet Explorer Security Update (129102)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-JUL
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19400
Remediation KB(s): KB4507434,KB4507448

MS21-OCT: Microsoft Windows Security Update (146693)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-OCT
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20143
Remediation KB(s): KB5006729,KB5006714

MS18-JAN: Microsoft Internet Explorer Security Update (MELTDOWN) (123602)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-JAN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18860
Remediation KB(s): KB4056568

MS19-SEP: Microsoft Internet Explorer Out-of-Band Security Update (129724)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-SEP
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19467
Remediation KB(s): KB4522007

MS19-OCT: Microsoft Internet Explorer Security Update (129805)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-OCT
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19507
Remediation KB(s): KB4520005,KB4519974

MS17-MAY: Microsoft Internet Explorer Security Update (122153) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS17-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18666
Remediation KB(s): KB4019215,KB4018271

MS18-DEC: Microsoft Internet Explorer Security Update (127240) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS18-DEC
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19203
Remediation KB(s): KB4483187,KB4471320,KB4470199

MS16-001: Cumulative Security Update for Internet Explorer (118689) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS16-001
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18161

MS19-FEB: Microsoft Internet Explorer Security Update (128001) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS19-FEB
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19267
Remediation KB(s): KB4486474,KB4487000

MS20-AUG: Microsoft Internet Explorer Security Update (138006) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS20-AUG
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19781
Remediation KB(s): KB4571687,KB4571703

MS17-OCT: Microsoft Internet Explorer Security Update (122637) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS17-OCT Vulnerable Path: C:\windows\system32\mshtml.dll File Version: 11.0.9600.17416 Fixed Version: 11.0.9600.18817 Remediation KB(s): KB4040685,KB4041693			
MS19-AUG: Microsoft Internet Explorer Security Update (129475) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS19-AUG Vulnerable Path: C:\windows\system32\mshtml.dll File Version: 11.0.9600.17416 Fixed Version: 11.0.9600.19431 Remediation KB(s): KB4512488,KB4511872		
MS17-SEP: Microsoft Internet Explorer Security Update (122554) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS17-SEP Vulnerable Path: C:\windows\system32\mshtml.dll File Version: 11.0.9600.17416 Fixed Version: 11.0.9600.18792 Remediation KB(s): KB4038792,KB4036586		
MS19-SEP: Microsoft Internet Explorer Security Update (129632) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS19-SEP Vulnerable Path: C:\windows\system32\mshtml.dll File Version: 11.0.9600.17416 Fixed Version: 11.0.9600.19463 Remediation KB(s): KB4516046,KB4516067		
MS16-118: Cumulative Security Update for Internet Explorer (121027) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS16-118 Vulnerable Path: C:\windows\system32\mshtml.dll File Version: 11.0.9600.17416 Fixed Version: 11.0.9600.18500		
MS18-OCT: Microsoft Internet Explorer Security Update (126601) **internal | explicit | OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS18-OCT Vulnerable Path: C:\windows\system32\mshtml.dll File Version: 11.0.9600.17416 Fixed Version: 11.0.9600.19155 Remediation KB(s): KB4462949,KB4462926		
MS20-JAN: Microsoft Internet Explorer Security Update (132229) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-JAN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19597
Remediation KB(s): KB4534297,KB4534251

MS21-MAY: Microsoft Internet Explorer Security Update (144993)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS21-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.20016
Remediation KB(s): KB5003165,KB5003209

MS18-JUN: Microsoft Internet Explorer Security Update (125543)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS18-JUN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19036
Remediation KB(s): KB4230450,KB4284815

MS16-095: Cumulative Security Update for Internet Explorer (119722)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS16-095
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18427

MS19-NOV: Microsoft Internet Explorer Security Update (131730)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS19-NOV
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19541
Remediation KB(s): KB4525106,KB4525243

MS18-SEP: Microsoft Internet Explorer Security Update (126400)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS18-SEP
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19130
Remediation KB(s): KB4457426,KB4457129

MS19-APR: Microsoft Internet Explorer Security Update (128575)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS19-APR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19326
Remediation KB(s): KB4493446,KB4493435

MS20-FEB: Microsoft Internet Explorer Security Update (132515) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-FEB
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19626
Remediation KB(s): KB4537767,KB4537821

MS20-MAR: Microsoft Internet Explorer Security Update (132714) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19650
Remediation KB(s): KB4540671,KB4541509

MS20-MAY: Microsoft Internet Explorer Security Update (133999) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19699
Remediation KB(s): KB4556798,KB4556846

MS17-APR: Microsoft .NET Security Update (122049) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS17-APR
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.drawing.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36366
Remediation KB(s): KB4014983

MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (117380) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS15-010
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17630

MS21-OCT: Microsoft Internet Explorer Security Update (146692) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-OCT
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.20139
Remediation KB(s): KB5006714,KB5006671

MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution (118131)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-082
Vulnerable Path: C:\windows\system32\mstscax.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17931

MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege (117224)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-004
Vulnerable Path: C:\windows\system32\tswbprxy.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17555

MS15-092: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (118121)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-092
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17933

MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (117733)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-048
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.security.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.34248

MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution (117875)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-060
Vulnerable Path: C:\windows\system32\comctl32.dll
File Version: 5.82.9600.17415
Fixed Version: 5.82.9600.17810

MS16-076: Security Update for Netlogon (119496)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS16-076
Vulnerable Path: C:\windows\system32\wdigest.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18334

MS17-NOV: Microsoft Windows Security Update (122792)

N/A / tcp Medium

internal | **explicit** | **OS auth**

unknown

Missing Microsoft Patch: MS17-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18838
Remediation KB(s): KB4048961,KB4048958

MS19-JAN: Microsoft Internet Explorer Security Update (127738)

N/A / tcp Medium

internal | **explicit** | **OS auth**

unknown

Missing Microsoft Patch: MS19-JAN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19236
Remediation KB(s): KB4480963,KB4480965

MS16-077: Security Update for WPAD (119495)

N/A / tcp Medium

internal | **explicit** | **OS auth**

unknown

Missing Microsoft Patch: MS16-077
Vulnerable Path: C:\windows\system32\drivers\netbt.sys
File Version: 6.3.9600.16384
Fixed Version: 6.3.9600.18340

MS16-061: Security Update for Microsoft RPC (119356)

N/A / tcp Medium

internal | **explicit** | **OS auth**

unknown

Missing Microsoft Patch: MS16-061
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18233

MS18-JAN: Microsoft .NET Security Update (123656)

N/A / tcp Medium

internal | **explicit** | **OS auth**

unknown

Missing Microsoft Patch: MS18-JAN
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.servicemodel.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36427
Remediation KB(s): KB4054993,KB4054170

MS16-114: Security Update for Windows SMBv1 Server (120908)

N/A / tcp Medium

internal | **explicit** | **OS auth**

unknown

Missing Microsoft Patch: MS16-114
Vulnerable Path: C:\windows\system32\drivers\srv.sys
File Version: 6.3.9600.17238
Fixed Version: 6.3.9600.18432

MS17-AUG: Microsoft Internet Explorer Security Update (122396)

N/A / tcp Medium

internal | explicit | OS auth

unknown

Missing Microsoft Patch: MS17-AUG
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18763
Remediation KB(s): KB4034733

MS18-JUL: Microsoft .NET Security Update (125658)

N/A / tcp Medium

internal | explicit | OS auth

unknown

Missing Microsoft Patch: MS18-JUL
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.identitymodel.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36450
Remediation KB(s): KB4338600,KB4338415

MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (118683)

N/A / tcp Medium

internal | explicit | OS auth

unknown

Missing Microsoft Patch: MS16-007
Vulnerable Path: C:\windows\system32\advapi32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18155

MS16-072: Security Update for Group Policy (119500)

N/A / tcp Medium

internal | explicit | OS auth

unknown

Missing Microsoft Patch: MS16-072
Vulnerable Path: C:\windows\system32\gpsvc.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18339

MS16-034: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (119083)

N/A / tcp Medium

internal | explicit | OS auth

unknown

Missing Microsoft Patch: MS16-034
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18228

MS16-149: Security Update for Windows (121322)

N/A / tcp Medium

internal | explicit | OS auth

unknown

Missing Microsoft Patch: MS16-149
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS16-080: Security Update for Microsoft Windows PDF (119492)

N/A / tcp Medium

internal | explicit | OS auth

unknown

Missing Microsoft Patch: MS16-080
Vulnerable Path: C:\windows\system32\glcndfilter.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18336

MS16-060: Security Update for Windows Kernel (119357)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-060
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18233

MS16-048: Security Update for CSRSS (119268)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-048
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18258

MS16-134: Security Update for Common Log File System Driver (121128)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-134
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18524

MS16-074: Security Update for Microsoft Graphics Component (119498)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-074
Vulnerable Path: C:\windows\system32\gdi32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18344

MS16-151: Security Update for Kernel-Mode Driver (121320)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-151
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (118982)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-014
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18192

MS16-135: Security Update for Windows Kernel-Mode Drivers (121127)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-135
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18524

MS17-017: Security Update for Windows Kernel (121899)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-017
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18603

MS16-073: Security Update for Windows Kernel-Mode Drivers (119499)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-073
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18340

MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (119085)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-032
Vulnerable Path: C:\windows\system32\seclogon.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18230

MS16-018: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (118978)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-018
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18190

MS15-030: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (117467)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-030
Vulnerable Path: C:\windows\system32\rdpudd.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17667

MS17-018: Security Update for Windows Kernel-Mode Drivers (121898)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-018
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18603

MS15-007: Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service (117221)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-007
Vulnerable Path: C:\windows\system32\iassam.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17549

MS16-075: Security Update for Windows SMB Server (119497)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-075
Vulnerable Path: C:\windows\system32\lsasrv.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18298

MS18-MAY: Microsoft .NET Security Update (124370)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS18-MAY
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.security.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36440
Remediation KB(s): KB4095876,KB4095517

MS16-090: Security Update for Windows Kernel-Mode Drivers (119627)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-090
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18377

MS18-JAN: Microsoft Windows Security Update (MELTDOWN) (123603)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS18-JAN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18872
Remediation KB(s): KB4056898

MS16-111: Security Update for Windows Kernel (120911)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-111
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18438

MS17-JUN: Microsoft Internet Explorer Security Update (122280)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-JUN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18698
Remediation KB(s): KB4022726,KB4021558

MS18-NOV: Microsoft Internet Explorer Security Update (126948)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS18-NOV
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19180
Remediation KB(s): KB4467697,KB4466536

MS16-008: Security Update for Windows Kernel to Address Elevation of Privilege (118682)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-008
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18185

MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (117582)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-038
Vulnerable Path: C:\windows\system32\drivers\clfs.sys
File Version: 6.3.9600.17055
Fixed Version: 6.3.9600.17719

MS15-133: Security Update for Windows PGM to Address Elevation of Privilege (118661)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-133
Vulnerable Path: C:\windows\system32\drivers\rmcast.sys
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18119

MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (117225)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-003
Vulnerable Path: C:\windows\system32\profsvc.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17552

MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (117227)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-001
Vulnerable Path: C:\windows\system32\drivers\ahcache.sys
File Version: 6.3.9600.16384
Fixed Version: 6.3.9600.17555

MS15-119: Security Update for Winsock to Address Elevation of Privilege (118492)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-119
Vulnerable Path: C:\windows\system32\drivers\afd.sys
File Version: 6.3.9600.17194
Fixed Version: 6.3.9600.18089

MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (118251)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-102
Vulnerable Path: C:\windows\system32\schedsvc.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18001

MS15-015: Vulnerability in Microsoft Windows Could Allow Elevation of Privilege (117375)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-015
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17630

MS15-061: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (117874)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-061
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17837

MS15-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (117472)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-025
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17668

MS15-072: Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (118043)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-072
Vulnerable Path: C:\windows\system32\gdi32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17902

MS15-073: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (118042)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-073
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17915

MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (118662)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-132
Vulnerable Path: C:\windows\system32\comsvcs.dll
File Version: 2001.12.10530.17415
Fixed Version: 2001.12.10530.18146

MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (117730)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-051
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17796

MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (118039)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-076
Vulnerable Path: C:\windows\system32\lsasrv.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17918

MS15-023: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (117474)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-023
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17694

MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege (118128)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-085
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17936

MS15-077: Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (118038)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-077
Vulnerable Path: C:\windows\system32\atmfd.dll
File Version: 5.1.2.238
Fixed Version: 5.1.2.242

MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege (117731)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-050
Vulnerable Path: C:\windows\system32\services.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17793

MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (119084)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS16-033
Vulnerable Path: C:\windows\system32\drivers\usbstor.sys
File Version: 6.3.9600.17331
Fixed Version: 6.3.9600.18224

MS15-120: Security Update for IPSec to Address Denial of Service (118491)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-120
Vulnerable Path: C:\windows\system32\bfe.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18009

MS16-112: Security Update for Windows Lock Screen (120910) **internal | explicit | OS auth**	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS16-112
Vulnerable Path: C:\windows\system32\pnidui.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18434

MS16-138: Security Update to Microsoft Virtual Hard Drive (121124) **internal | explicit | OS auth**	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS16-138
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18525

MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass (117223) **internal | explicit | OS auth**	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS15-005
Vulnerable Path: C:\windows\system32\nlasvc.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17550

MS17-016: Security Update for Windows IIS (121900) **internal | explicit | OS auth**	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS17-016
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18603

MS15-121: Security Update for Schannel to Address Spoofing (118490) **internal | explicit | OS auth**	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS15-121
Vulnerable Path: C:\windows\system32\schannel.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18088

MS19-MAY: Microsoft .NET Security Update (128800) **internal | explicit | OS auth**	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS19-MAY
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\mscorlib.dll
File Version: 4.0.30319.34014
Fixed Version: 4.0.30319.36543
Remediation KB(s): KB4498963,KB4499408

MS16-153: Security Update for Common Log File System Driver (121318) **internal | explicit | OS auth**	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS16-153
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service (118975)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS16-021
Vulnerable Path: C:\windows\system32\iassam.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18191

MS17-MAY: Microsoft .NET Security Update (122158)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS17-MAY
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.data.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36372
Remediation KB(s): KB4019114

MS15-055: Vulnerability in Schannel Could Allow Information Disclosure (117726)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-055
Vulnerable Path: C:\windows\system32\schannel.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17810

MS14-085: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (117082)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS14-085
Vulnerable Path: C:\windows\system32\windowscodecs.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17483

MS16-082: Security Update for Microsoft Windows Search Component (119490)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS16-082
Vulnerable Path: C:\windows\system32\structuredquery.dll
File Version: 7.0.9600.17415
Fixed Version: 7.0.9600.18334

MS15-075: Vulnerabilities in OLE Could Allow Elevation of Privilege (118040)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-075
Vulnerable Path: C:\windows\system32\ole32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17905

MS15-122: Security Update for Kerberos to Address Security Feature Bypass (118489) N/A / tcp unknown Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-122
Vulnerable Path: C:\windows\system32\kerberos.dll
File Version: 6.3.9600.17340
Fixed Version: 6.3.9600.18091

MS16-092: Security Update for Windows Kernel (119625) N/A / tcp unknown Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS16-092
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18233

MS15-052: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (117729) N/A / tcp unknown Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-052
Vulnerable Path: C:\windows\system32\drivers\cng.sys
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17785

MS17-022: Security Update for Microsoft XML Core Services (121894) N/A / tcp unknown Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS17-022
Vulnerable Path: C:\windows\system32\msxml3.dll
File Version: 8.110.9600.17415
Fixed Version: 8.110.9600.18574

MS16-065: Security Update for .NET Framework (119353) N/A / tcp unknown Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS16-065
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.dll
File Version: 4.0.30319.34003
Fixed Version: 4.0.30319.34293

MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure (118129) N/A / tcp unknown Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-084
Vulnerable Path: C:\windows\system32\msxml3.dll
File Version: 8.110.9600.17415
Fixed Version: 8.110.9600.17931

MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure (118125)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-088
Vulnerable Path: C:\windows\system32\notepad.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17930

MS15-027: Vulnerability in NETLOGON Could Allow Spoofing (117470)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-027
Vulnerable Path: C:\windows\system32\netlogon.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17678

MS15-031: Vulnerability in Schannel Could Allow Security Feature Bypass (117466)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-031
Vulnerable Path: C:\windows\system32\schannel.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17702

MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (117468)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-029
Vulnerable Path: C:\windows\system32\wmphoto.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17668

MS15-016: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (117374)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-016
Vulnerable Path: C:\windows\system32\windowscodecs.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17631

MS15-071: Vulnerability in Netlogon Could Allow Elevation of Privilege (118044)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-071
Vulnerable Path: C:\windows\system32\netlogon.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17901

MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass (117376)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-014
Vulnerable Path: C:\windows\system32\scesrv.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17552

MS17-021: Security Update for Windows DirectShow (121895)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-021
Vulnerable Path: C:\windows\system32\quartz.dll
File Version: 6.6.9600.17415
Fixed Version: 6.6.9600.18569

MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure (117579)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-041
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.web.dll
File Version: 4.0.30319.34009
Fixed Version: 4.0.30319.34248

MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (117469)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-028
Vulnerable Path: C:\windows\system32\ubpm.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17671

MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass (117222)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-006
Vulnerable Path: C:\windows\system32\wer.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17550

SMB Security Signatures Not Required (104188)

internal | **explicit** | **unauth**

139 / tcp
netbios

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

Content Security Policy Missing (148043) — 80 / tcp — Trivial

internal | explicit | unauth — http

Missing Content Security Policy.

Content Security Policy Missing (148043) — 8530 / tcp — Trivial

internal | explicit | unauth — http

Missing Content Security Policy.

Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (120681) — N/A / tcp — Trivial

internal | compliance | CIS auth — unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (120621) — N/A / tcp — Trivial

internal | compliance | CIS auth — unknown

Expected: 0
Collected: 3
Result: FAIL

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (120803) — N/A / tcp — Trivial

internal | compliance | CIS auth — unknown

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (120710) — N/A / tcp — Trivial

internal | compliance | CIS auth — unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (120700) — N/A / tcp — Trivial

internal | compliance | CIS auth — unknown

Expected: <= 90
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Account Lockout' is set to 'Success' (120667)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (120658)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (120582)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (120610)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Link Local Multicast Name Resolution (LLMNR) Enabled (129962)

internal | recon | OS auth

N/A / tcp
unknown

Trivial

LLMNR is enabled

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' (120771)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (120592)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120554)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-271721585-897601226-2024613209-625570482-296978595,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
Result: FAIL

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (120779)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (120651)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'EMET 5.5' or higher is installed (120755)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (120659)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (120808)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (120738)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (120815)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (120642)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (120562)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (120813)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (120519)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 14
Collected: 0
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (120591)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (120754) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (120683) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: C:\Program Files\LAPS\CSE\AdmPwd.dll Collected: Not Defined Result: FAIL		
Compliance: Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (120762) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 2 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (120760) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 3 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (120617) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (120524) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: >= 15 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallpublicfw.log' (120653) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: %systemroot%\system32\logfiles\firewall\publicfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Shut down the system' is set to 'Administrators' (120556) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (120575) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120825) N/A / tcp unknown Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges
Result: PASS

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (120677) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (120715) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (120749) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (120811)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (120631)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (120712)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120764)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent the usage of SkyDrive for file storage' is set to 'Enabled' (120792)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (120577)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (120662)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (120585) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (120578) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (120718) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: PASS

Compliance: Ensure 'Profile single process' is set to 'Administrators' (120552) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120765) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (120599) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (120655)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (120670)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Default Protections for Popular Software' is set to 'Enabled' (120758)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Popular Software
Result: FAIL

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (120550)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (120799)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (120531)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (120820)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen
Result: PASS

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (120523)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120613)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (120685)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (120618)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (120628)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (120560)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (120532) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (120574) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Process Creation' is set to 'Success' (120664) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (120525) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (120530) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (120682) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (120774) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (120743) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password protect the screen saver' is set to 'Enabled' (120818) N/A / tcp unknown Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Control Panel\Personalization\Password protect the screen saver
Result: PASS

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (120602) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (120661) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (120638) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (120597) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (120734)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (120652)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (120736)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable screen saver' is set to 'Enabled' (120816)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver
Result: PASS

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (120576)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (120648)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Modify an object label' is set to 'No One' (120549)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (120568)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (120737)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths and sub-paths' (120601)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

[Large data section omitted]

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (120587)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (120757)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: *\Internet Explorer\iexplore.exe
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (120520)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (120559)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (120819)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Screen saver timeout: Seconds
Result: PASS

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (120521)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (120713)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (120612)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 1
Collected: 1
Result: PASS

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disa... (120691)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (120805)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (120794) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Accounts: Rename administrator account' (120563) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: not Administrator
Collected: Administrator
Result: FAIL

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (120705) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

CIS Benchmark Profile (116437) N/A / tcp unknown Trivial

internal | compliance | OS auth

CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0:SERVER

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (120589) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (120551) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit Security State Change' is set to 'Success' (120678) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (120741)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (120528)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,S-1-5-82-271721585-897601226-2024613209-625570482-296978595,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
Result: FAIL

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (120566)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (120590)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session
Result: FAIL

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (120561)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120654)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (120626)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (120689)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (120753)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (120817)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Force specific screen saver: Screen saver executable name
Result: PASS

Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (120742)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

IPv6 Enabled (142306)

N/A / tcp
unknown

Trivial

internal | **explicit** | **OS auth**

IPv6 enabled on network interfaces with the following IPv4 addresses

192.168.68.54

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (120544)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (120776) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (120696) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (120526) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (120632) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (120595) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (120680) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Audit Logoff' is set to 'Success' (120668) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (120645)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120614)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (120534)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120634)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (120542)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (120787)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a service' to include 'Guests' (120539) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (120607) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (120687) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (120646) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (120586) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1 or 2 or 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (120555) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Create a token object' is set to 'No One' (120533) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (120641)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (120756)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (120635)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (120625)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120768)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (120636)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely... (120690) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 2 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (120788) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (120594) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: >= 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (120605) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (120573) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (120772) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (120517)

internal | compliance | CIS auth

N/A / tcp

unknown

Trivial

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
Result: FAIL

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (120616)

internal | compliance | CIS auth

N/A / tcp

unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (120640)

internal | compliance | CIS auth

N/A / tcp

unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120806)

internal | compliance | CIS auth

N/A / tcp

unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (120584)

internal | compliance | CIS auth

N/A / tcp

unknown

Trivial

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration
Result: PASS

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120810)

internal | compliance | CIS auth

N/A / tcp

unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Create symbolic links' (120536)

internal | compliance | CIS auth

N/A / tcp

unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (120706) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
Result: FAIL

Compliance: Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (120798) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (120676) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120801) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (120620) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 2
Collected: 0
Result: FAIL

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (120672) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (120649)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (120604)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (120675)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (120804)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (120619)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (120759)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software
Result: FAIL

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (120538)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (120516)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 24
Collected: 0
Result: FAIL

Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (120686)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120769)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (120824)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile.
Result: PASS

Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (120545)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (120639)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewalldomainfw.log' (120633)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (120714)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Debug programs' is set to 'Administrators' (120537)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (120766)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 196608
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (120800)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (120558)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (120663)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (120624)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120809)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (120627)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (120572)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Configure 'Accounts: Rename guest account' (120564)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: not Guest
Collected: Guest
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (120656)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (120581) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: Any text Collected: Empty string Result: FAIL		
Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (120593) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (120579) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: 1 Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (120629) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (120596) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (120553) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: Administrators,NT SERVICE\\WdiServiceHost Collected: ADMINISTRATORS,NT SERVICE\WdiServiceHost Result: PASS		
Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (120603) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: No Defined Values
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (120716) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (120673) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (120529) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (120518) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: >= 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (120608) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 2147483644
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Lock pages in memory' is set to 'No One' (120546) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (120622)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (120522)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (120814)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (120688)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 30
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (120704)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120763)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (120692)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (120630)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (120735)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (120761)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (120694)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (120750)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (120789)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (120565)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (120637)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Special Logon' is set to 'Success' (120671)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (120751)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (120669)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (120567)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (120647) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (120623) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120770) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallprivatefw.log' (120643) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120807) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (120606) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (120684)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (120611)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (120609)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (120657)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (120783)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths' (120600)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Collected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Result: PASS

Compliance: Ensure 'Deny log on locally' to include 'Guests' (120540) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (120580) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
Result: FAIL

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (120782) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120644) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120767) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (120790) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (120679) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (120752)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 255
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Manage auditing and security log' (120548)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (120795)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (120674)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (120588)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (120717)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (120822)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments
Result: PASS

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (120784)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (120823)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments
Result: PASS

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (120697)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: <= 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (120773)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (120650)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (120535)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120543)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-271721585-897601226-2024613209-625570482-296978595,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
Result: FAIL

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (120615)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Default IIS Webpage Detected (117366)
internal | recon | unauth

80 / tcp
http

Trivial

Default IIS Webpage Detected

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (120541)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

WIN-30QQRC10MGG D

IP: 192.168.68.54
Asset name: WIN-30QQRC10MGG
Operating system: Windows Server 2012 R2
Asset type: Server

Protocol	Service
http	80 / tcp
ntp	123 / udp
msrpc	135 / tcp
unknown	137 / udp

netbios-ns	137 / udp
unknown	138 / udp
netbios	139 / tcp
smb	445 / tcp
unknown	500 / udp
unknown	554 / tcp
unknown	559 / tcp
unknown	1935 / tcp
unknown	4500 / udp
winrm	5985 / tcp
unknown	6667 / tcp
http	8530 / tcp
unknown	9443 / tcp
unknown	9998 / tcp
http	9999 / tcp
unknown	10000 / tcp
unknown	17185 / udp
unknown	32774 / udp
unknown	49152 / tcp
unknown	49153 / tcp
dcerpc	49154 / tcp
dcerpc	49155 / tcp
dcerpc	49156 / tcp
dcerpc	49180 / tcp
dcerpc	49206 / tcp

unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Success	N/A	Success	N/A

Authenticated Scan Credentials Used Successfully
OS: Threat Domain **CIS:** Threat Domain

Vulnerability Title	Service(s)	Severity
MS19-FEB: Microsoft Windows Security Update (127998) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS19-FEB Vulnerable Path: C:\windows\system32\jscript.dll File Version: 5.8.9600.17416 Fixed Version: 5.8.9600.19267 Remediation KB(s): KB4487028,KB3173424,KB4487000		
MS20-JUL: Microsoft Windows Security Update (137512) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS20-JUL Vulnerable Path: C:\windows\system32\windowscodecs.dll File Version: 6.3.9600.17415 Fixed Version: 6.3.9600.19749 Remediation KB(s): KB4565540,KB4565541,KB4566425		
MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) (117590) **internal** | **explicit** | **unauth**	80 / tcp http	High
[Large data section omitted]		
MS19-OCT: Microsoft Windows Security Update (129806) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High
Missing Microsoft Patch: MS19-OCT Vulnerable Path: C:\windows\system32\jscript.dll File Version: 5.8.9600.17416 Fixed Version: 5.8.9600.19507 Remediation KB(s): KB4512938,KB4520005,KB4519990		
MS20-MAY: Microsoft Windows Security Update (134000) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-MAY
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19697
Remediation KB(s): KB4556853,KB4556846

MS20-DEC: Microsoft Windows Security Update (143512) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-DEC
Vulnerable Path: C:\windows\system32\localspl.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19893
Remediation KB(s): KB4592484,KB4592495

MS21-JUL: Microsoft Windows Security Update (145614) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-JUL
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20069
Remediation KB(s): KB5004954,KB5004233,KB5004958,KB5004285,KB5004298

MS19-NOV: Microsoft Windows Security Update (131731) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS19-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19538
Remediation KB(s): KB4525243,KB4524445,KB4525250

MS21-MAY: Microsoft Windows Security Update (144994) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-MAY
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20017
Remediation KB(s): KB5003220,KB5003209

MS21-SEP: Microsoft Windows Security Update (146370) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-SEP
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20117
Remediation KB(s): KB5005613,KB5005627

MS19-AUG: Microsoft Windows Security Update (129476) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS19-AUG
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19427
Remediation KB(s): KB4512489,KB4512488

MS21-AUG: Microsoft Windows Security Update (146090) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-AUG
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20094
Remediation KB(s): KB5005106,KB5005076

MS19-MAR: Microsoft Windows Security Update (128290) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS19-MAR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19304
Remediation KB(s): KB4489881,KB4489883,KB3173424

MS20-NOV: Microsoft Windows Security Update (143189) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19867
Remediation KB(s): KB4586823,KB4586845

MS17-DEC: Microsoft Windows Security Update (123544) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS17-DEC
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18872
Remediation KB(s): KB4054522,KB4054519

MS18-OCT: Microsoft Windows Security Update (126602) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-OCT
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19153
Remediation KB(s): KB4462926,KB4462941

MS19-MAY: Microsoft Windows Security Update (ZombieLoad) (128795) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS19-MAY
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19355
Remediation KB(s): KB3173424,KB4499151,KB4499165

MS22-MAY: Microsoft Windows Security Update (148572)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-MAY
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20369
Remediation KB(s): KB5014001,KB5014011

MS20-MAR: Microsoft Windows Security Update (132715)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-MAR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19650
Remediation KB(s): KB4541509,KB4541505

MS18-JUL: Microsoft Windows Security Update (125654)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-JUL
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19064
Remediation KB(s): KB4338824,KB4338815

MS20-OCT: Microsoft Windows Security Update (142682)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-OCT
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19846
Remediation KB(s): KB4580347,KB4580358

MS21-DEC: Microsoft Windows Security Update (147272)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-DEC
Vulnerable Path: C:\windows\system32\spoolsv.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20201
Remediation KB(s): KB5008263,KB5008285

MS20-APR: Microsoft Windows Security Update (133731)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19670
Remediation KB(s): KB4550970,KB4550961

MS19-APR: Microsoft Windows Security Update (128576)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19328
Remediation KB(s): KB3173424,KB4493467,KB4493446

MS22-APR: Microsoft Windows Security Update (148319)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-APR
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20334
Remediation KB(s): KB5012670,KB5012639

MS21-JUN: Microsoft Windows Security Update (145281)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-JUN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20036
Remediation KB(s): KB5003671,KB5003636,KB5003681

MS17-SEP: Microsoft Windows Security Update (122555)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-SEP
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18790
Remediation KB(s): KB4038793,KB4038792

MS17-OCT: Microsoft Windows Security Update (122638)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-OCT
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18818
Remediation KB(s): KB4041693,KB4041687

MS22-JUN: Microsoft Windows Security Update (148994)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS22-JUN
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20396
Remediation KB(s): KB5014738,KB5014746

MS21-MAR: Microsoft Windows Security Update (144194) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS21-MAR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19968
Remediation KB(s): KB5000848,KB5000853

MS18-DEC: Microsoft Windows Security Update (127241) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS18-DEC
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19208
Remediation KB(s): KB4471320,KB4471322,KB3173424

MS21-APR: Microsoft Windows Security Update (144750) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS21-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19990
Remediation KB(s): KB5001393,KB5001382

MS19-JAN: Microsoft Windows Security Update (127739) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS19-JAN
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19236
Remediation KB(s): KB3173424,KB4480963,KB4480964

MS19-JUL: Microsoft Windows Security Update (129103) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS19-JUL
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19402
Remediation KB(s): KB4507457,KB4504418,KB4507448

MS17-JUN: Microsoft Windows Security Update (122281) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS17-JUN
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18696
Remediation KB(s): KB4022726,KB4022717

MS21-FEB: Microsoft Windows Security Update (144007) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-FEB
Vulnerable Path: C:\windows\system32\localspl.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19941
Remediation KB(s): KB4601349,KB4601384

MS17-JUL: Microsoft Windows Security Update (122296) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS17-JUL
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18737
Remediation KB(s): KB4025333,KB4025336

MS18-NOV: Microsoft Windows Security Update (126949) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19176
Remediation KB(s): KB4467703,KB3173424,KB4467697

MS22-JAN: Microsoft Windows Security Update (147420) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS22-JAN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20239
Remediation KB(s): KB5009595,KB5009624

MS20-JAN: Microsoft Windows Security Update (132230) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-JAN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19593
Remediation KB(s): KB4534297,KB4534309

MS21-JAN: Microsoft Windows Security Update (143778) **internal** | **explicit** | **OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-JAN
Vulnerable Path: C:\windows\system32\localspl.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19920
Remediation KB(s): KB4598285,KB4598275

MS19-SEP: Microsoft Windows Security Update (129633)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-SEP
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19457
Remediation KB(s): KB4516067,KB4516064,KB4512938

MS21-NOV: Microsoft Windows Security Update (146938)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20165
Remediation KB(s): KB5007255,KB5007247

MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (118133)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS15-080
Vulnerable Path: C:\windows\system32\atmfd.dll
File Version: 5.1.2.238
Fixed Version: 5.1.2.245

MS15-124: Cumulative Security Update for Internet Explorer (118670)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS15-124
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18125

MS15-009: Security Update for Internet Explorer (117381)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS15-009
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17631

MS17-010: Security Update for Microsoft Windows SMB Server (121906)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: ms17-010
Vulnerable Path: C:\windows\system32\drivers\srv.sys
File Version: 6.3.9600.17238
Fixed Version: 6.3.9600.18604

MS15-032: Cumulative Security Update for Internet Explorer (117588) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS15-032
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17728

MS15-106: Cumulative Security Update for Internet Explorer (118394) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS15-106
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18052

MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (117737) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS15-044
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17796

MS15-079: Cumulative Security Update for Internet Explorer (118134) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS15-079
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17937

MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (118096) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS15-078
Vulnerable Path: C:\windows\system32\atmfd.dll
File Version: 5.1.2.238
Fixed Version: 5.1.2.243

MS15-093: Security Update for Internet Explorer (118245) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS15-093
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17963

MS15-056: Cumulative Security Update for Internet Explorer (117878)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-056
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17842

MS15-021: Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (117476)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-021
Vulnerable Path: C:\windows\system32\atmfd.dll
File Version: 5.1.2.238
Fixed Version: 5.1.2.241

MS15-018: Cumulative Security Update for Internet Explorer (117479)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-018
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17690

MS15-043: Cumulative Security Update for Internet Explorer (117738)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-043
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17801

MS15-065: Security Update for Internet Explorer (118050)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-065
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.17905

MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege (116972)

N/A / tcp
unknown

High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS14-068
Vulnerable Path: C:\windows\system32\kerberos.dll
File Version: 6.3.9600.17340
Fixed Version: 6.3.9600.17423

MS21-JUL: Microsoft Windows Out-of-Band Security Update (145515)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-JUL
Vulnerable Path: C:\windows\system32\spoolsv.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20046
Remediation KB(s): KB5004954,KB5004958

MS20-APR: Microsoft Internet Explorer Security Update (133730)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-APR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19671
Remediation KB(s): KB4550905,KB4550961

MS19-DEC: Microsoft Windows Security Update (131867)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-DEC
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19574
Remediation KB(s): KB4530702,KB4524445,KB4530730

MS21-AUG: Microsoft Internet Explorer Security Update (146092)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-AUG
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19404
Remediation KB(s): KB5005036

MS18-APR: Microsoft Windows Security Update (123955)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18979
Remediation KB(s): KB4093114,KB4093115

MS20-JUN: Microsoft Windows Security Update (137200)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-JUN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19727
Remediation KB(s): KB4561673,KB4561666

MS22-JUL: Microsoft Windows Security Update (149222)

N/A / tcp
unknown
High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS22-JUL
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20475
Remediation KB(s): KB5015874,KB5015877

MS20-FEB: Microsoft Windows Security Update (132516)

N/A / tcp
unknown
High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS20-FEB
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19630
Remediation KB(s): KB4502496,KB4537803,KB4537821

MS16-040: Security Update for Microsoft XML Core Services (119275)

N/A / tcp
unknown
High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS16-040
Vulnerable Path: C:\windows\system32\msxml3.dll
File Version: 8.110.9600.17415
Fixed Version: 8.110.9600.18258

MS22-FEB: Microsoft Windows Security Update (147753)

N/A / tcp
unknown
High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS22-FEB
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20269
Remediation KB(s): KB5010419,KB5010395

MS18-SEP: Microsoft Windows Security Update (126401)

N/A / tcp
unknown
High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS18-SEP
Vulnerable Path: C:\windows\system32\windowscodecs.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19133
Remediation KB(s): KB4457143,KB4457129

MS16-144: Cumulative Security Update for Internet Explorer (121327)

N/A / tcp
unknown
High

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS16-144
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS16-063: Cumulative Security Update for Internet Explorer (119505) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS16-063
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18349

MS20-SEP: Microsoft Internet Explorer Security Update (138218) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS20-SEP
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19811
Remediation KB(s): KB4577066,KB4577010

MS19-MAY: Microsoft Internet Explorer Security Update (128794) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS19-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19355
Remediation KB(s): KB4498206,KB4499151

MS20-SEP: Microsoft Windows Security Update (138219) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS20-SEP
Vulnerable Path: C:\windows\system32\puiobj.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19810
Remediation KB(s): KB4577071,KB4577066

MS16-146: Security Update for Microsoft Graphics Component (121325) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS16-146
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS20-AUG: Microsoft Windows Security Update (138007) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS20-AUG
Vulnerable Path: C:\windows\system32\puiobj.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.19785
Remediation KB(s): KB4571723,KB4571703

MS22-MAR: Microsoft Windows Security Update (148037) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS22-MAR
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.20302
Remediation KB(s): KB5011564,KB5011560

MS16-132: Security Update for Microsoft Graphics Component (121130) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS16-132
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18524

MS19-JUN: Microsoft Windows Security Update (128962) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS19-JUN
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19377
Remediation KB(s): KB4503276,KB4503290,KB3173424

MS18-APR: Microsoft Internet Explorer Security Update (123954) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-APR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18978
Remediation KB(s): KB4092946,KB4093114

MS18-MAY: Microsoft Internet Explorer Security Update (124365) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19003
Remediation KB(s): KB4103768,KB4103725

MS18-AUG: Microsoft Windows Security Update (125932) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-AUG
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19095
Remediation KB(s): KB4343888,KB4343898

MS18-JUN: Microsoft Windows Security Update (125544)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-JUN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19000
Remediation KB(s): KB4284878,KB4284815

MS16-009: Cumulative Security Update for Internet Explorer (118985)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-009
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18205

MS16-147: Security Update for Microsoft Uniscribe (121324)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-147
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS16-104: Cumulative Security Update for Internet Explorer (120918)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-104
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18450

MS17-AUG: Microsoft Windows Security Update (122397)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-AUG
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18759
Remediation KB(s): KB4034672,KB4034681

MS18-MAY: Microsoft Windows Security Update (124366)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-MAY
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.19000
Remediation KB(s): KB4103725,KB4103715

MS18-AUG: Microsoft Internet Explorer Security Update (125931) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS18-AUG
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19101
Remediation KB(s): KB4343205,KB4343898

MS16-087: Security Update for Windows Print Spooler Components (119630) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS16-087
Vulnerable Path: C:\windows\system32\win32spl.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18398

MS17-MAY: Microsoft Windows Security Update (122154) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS17-MAY
Vulnerable Path: C:\windows\system32\urlmon.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18666
Remediation KB(s): KB4019215

MS20-NOV: Microsoft Internet Explorer Security Update (143188) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS20-NOV
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19867
Remediation KB(s): KB4586845,KB4586768

MS17-APR: Microsoft Windows Security Update (122045) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS17-APR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18623
Remediation KB(s): KB4015550

MS18-MAR: Microsoft Windows Security Update (123856) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS18-MAR
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18954
Remediation KB(s): KB4088876,KB4088879

MS18-FEB: Microsoft Windows Security Update (123788)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS18-FEB
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18907
Remediation KB(s): KB4074594,KB4074597

MS16-037: Cumulative Security Update for Internet Explorer (119278)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS16-037
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18281

MS21-SEP: Microsoft Internet Explorer Security Update (146369)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS21-SEP
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19404
Remediation KB(s): KB5005563,KB5005627,KB5005613

MS16-012: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (118984)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS16-012
Vulnerable Path: C:\windows\system32\glcndfilter.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18184

MS17-013: Security Update for Microsoft Graphics Component (121903)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS17-013
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18603

MS16-130: Security Update for Microsoft Windows (121132)

N/A / tcp
unknown

High

internal | explicit | OS auth

Missing Microsoft Patch: MS16-130
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18524

MS16-028: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (119089)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-028
Vulnerable Path: C:\windows\system32\glcndfilter.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18229

MS16-039: Security Update for Microsoft Graphics Component (119276)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-039
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18290

MS21-MAY: Microsoft Internet Explorer Security Update (144993)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.20016
Remediation KB(s): KB5003165,KB5003209

MS19-OCT: Microsoft Internet Explorer Security Update (129805)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-OCT
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19507
Remediation KB(s): KB4520005,KB4519974

MS18-JUN: Microsoft Internet Explorer Security Update (125543)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-JUN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19036
Remediation KB(s): KB4284815,KB4230450

MS17-SEP: Microsoft Internet Explorer Security Update (122554)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-SEP
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18792
Remediation KB(s): KB4036586,KB4038792

MS19-DEC: Microsoft Internet Explorer Security Update (131866)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-DEC
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19572
Remediation KB(s): KB4530702,KB4530677

MS19-APR: Microsoft Internet Explorer Security Update (128575)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-APR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19326
Remediation KB(s): KB4493446,KB4493435

MS16-118: Cumulative Security Update for Internet Explorer (121027)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-118
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18500

MS17-006: Cumulative Security Update for Internet Explorer (121910)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-006
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18618

MS21-OCT: Microsoft Windows Security Update (146693)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS21-OCT
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.20143
Remediation KB(s): KB5006714,KB5006729

MS20-AUG: Microsoft Internet Explorer Security Update (138006)
internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-AUG
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19781
Remediation KB(s): KB4571703,KB4571687

MS17-MAY: Microsoft Internet Explorer Security Update (122153) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS17-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18666
Remediation KB(s): KB4018271,KB4019215

MS17-APR: Microsoft Internet Explorer Security Update (122044) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS17-APR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18639
Remediation KB(s): KB4015550,KB4014661

MS16-001: Cumulative Security Update for Internet Explorer (118689) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS16-001
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18161

MS20-FEB: Microsoft Internet Explorer Security Update (132515) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS20-FEB
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19626
Remediation KB(s): KB4537821,KB4537767

MS19-NOV: Microsoft Internet Explorer Security Update (131730) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS19-NOV
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19541
Remediation KB(s): KB4525243,KB4525106

MS19-SEP: Microsoft Internet Explorer Security Update (129632) N/A / tcp High
internal | **explicit** | **OS auth** unknown

Missing Microsoft Patch: MS19-SEP
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19463
Remediation KB(s): KB4516067,KB4516046

MS18-OCT: Microsoft Internet Explorer Security Update (126601)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-OCT
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19155
Remediation KB(s): KB4462949,KB4462926

MS18-FEB: Microsoft Internet Explorer Security Update (123787)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-FEB
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18921
Remediation KB(s): KB4074736,KB4074594

MS20-JUN: Microsoft Internet Explorer Security Update (137199)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-JUN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19724
Remediation KB(s): KB4561603,KB4561666

MS19-JUL: Microsoft Internet Explorer Security Update (129102)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-JUL
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19400
Remediation KB(s): KB4507448,KB4507434

MS19-MAR: Microsoft Internet Explorer Security Update (128289)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19301
Remediation KB(s): KB4489873,KB4489881

MS18-JAN: Microsoft Internet Explorer Security Update (MELTDOWN) (123602)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

High

Missing Microsoft Patch: MS18-JAN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18860
Remediation KB(s): KB4056568

MS19-SEP: Microsoft Internet Explorer Out-of-Band Security Update (129724) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS19-SEP
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19467
Remediation KB(s): KB4522007

MS19-FEB: Microsoft Internet Explorer Security Update (128001) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS19-FEB
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19267
Remediation KB(s): KB4487000,KB4486474

MS19-AUG: Microsoft Internet Explorer Security Update (129475) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS19-AUG
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19431
Remediation KB(s): KB4511872,KB4512488

MS20-MAY: Microsoft Internet Explorer Security Update (133999) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-MAY
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19699
Remediation KB(s): KB4556798,KB4556846

MS18-DEC: Microsoft Internet Explorer Security Update (127240) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-DEC
Vulnerable Path: C:\windows\system32\jscript.dll
File Version: 5.8.9600.17416
Fixed Version: 5.8.9600.19203
Remediation KB(s): KB4470199,KB4471320,KB4483187

MS20-MAR: Microsoft Internet Explorer Security Update (132714) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS20-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19650
Remediation KB(s): KB4541509,KB4540671

MS18-SEP: Microsoft Internet Explorer Security Update (126400) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-SEP
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19130
Remediation KB(s): KB4457426,KB4457129

MS16-116: Security Update in OLE Automation for VBScript Scripting Engine (120906) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS16-116
Vulnerable Path: C:\windows\system32\oleaut32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18434

MS17-DEC: Microsoft Internet Explorer Security Update (123543) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS17-DEC
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18860
Remediation KB(s): KB4052978,KB4054519

MS17-NOV: Microsoft Internet Explorer Security Update (122791) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS17-NOV
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18817
Remediation KB(s): KB4048958,KB4047206

MS21-MAR: Microsoft Internet Explorer Security Update (144193) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS21-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19963
Remediation KB(s): KB5000800,KB5000848

MS18-JUL: Microsoft Internet Explorer Security Update (125653) **internal | explicit | OS auth**	N/A / tcp unknown	High

Missing Microsoft Patch: MS18-JUL
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19061
Remediation KB(s): KB4338815,KB4339093

MS20-JUL: Microsoft Internet Explorer Security Update (137511)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS20-JUL
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19750
Remediation KB(s): KB4565541,KB4565479

MS16-095: Cumulative Security Update for Internet Explorer (119722)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-095
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18427

MS19-JUN: Microsoft Internet Explorer Security Update (128961)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS19-JUN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19377
Remediation KB(s): KB4503276,KB4503259,KB4503290

MS17-JUL: Microsoft Internet Explorer Security Update (122295)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-JUL
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18739
Remediation KB(s): KB4025252,KB4025336

MS17-OCT: Microsoft Internet Explorer Security Update (122637)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS17-OCT
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18817
Remediation KB(s): KB4041693,KB4040685

MS16-023: Cumulative Security Update for Internet Explorer (119094)

internal | explicit | OS auth

N/A / tcp
unknown

High

Missing Microsoft Patch: MS16-023
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18231

MS18-MAR: Microsoft Internet Explorer Security Update (123855) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS18-MAR
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18953
Remediation KB(s): KB4089187,KB4088876

MS20-JAN: Microsoft Internet Explorer Security Update (132229) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS20-JAN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19597
Remediation KB(s): KB4534251,KB4534297

MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (117380) N/A / tcp High
unknown
internal | explicit | OS auth

Missing Microsoft Patch: MS15-010
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17630

MS17-APR: Microsoft .NET Security Update (122049) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS17-APR
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.drawing.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36366
Remediation KB(s): KB4014983

MS21-OCT: Microsoft Internet Explorer Security Update (146692) N/A / tcp High
internal | explicit | OS auth unknown

Missing Microsoft Patch: MS21-OCT
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.20139
Remediation KB(s): KB5006714,KB5006671

MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution (117875) N/A / tcp Medium
unknown
internal | explicit | OS auth

Missing Microsoft Patch: MS15-060
Vulnerable Path: C:\windows\system32\comctl32.dll
File Version: 5.82.9600.17415
Fixed Version: 5.82.9600.17810

MS15-092: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (118121)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-092
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17933

MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution (118131)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-082
Vulnerable Path: C:\windows\system32\mstscax.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17931

MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege (117224)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-004
Vulnerable Path: C:\windows\system32\tswbprxy.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17555

MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (117733)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-048
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.security.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.34248

MS16-077: Security Update for WPAD (119495)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS16-077
Vulnerable Path: C:\windows\system32\drivers\netbt.sys
File Version: 6.3.9600.16384
Fixed Version: 6.3.9600.18340

MS16-076: Security Update for Netlogon (119496)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS16-076
Vulnerable Path: C:\windows\system32\wdigest.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18334

MS17-AUG: Microsoft Internet Explorer Security Update (122396)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-AUG
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18763
Remediation KB(s): KB4034733

MS19-JAN: Microsoft Internet Explorer Security Update (127738)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS19-JAN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19236
Remediation KB(s): KB4480965,KB4480963

MS16-114: Security Update for Windows SMBv1 Server (120908)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-114
Vulnerable Path: C:\windows\system32\drivers\srv.sys
File Version: 6.3.9600.17238
Fixed Version: 6.3.9600.18432

MS18-JUL: Microsoft .NET Security Update (125658)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS18-JUL
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.identitymodel.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36450
Remediation KB(s): KB4338600,KB4338415

MS17-NOV: Microsoft Windows Security Update (122792)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-NOV
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18838
Remediation KB(s): KB4048958,KB4048961

MS18-JAN: Microsoft .NET Security Update (123656)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS18-JAN
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.servicemodel.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36427
Remediation KB(s): KB4054993,KB4054170

MS16-061: Security Update for Microsoft RPC (119356)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-061
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18233

MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution (118683)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-007
Vulnerable Path: C:\windows\system32\advapi32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18155

MS16-072: Security Update for Group Policy (119500)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-072
Vulnerable Path: C:\windows\system32\gpsvc.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18339

MS15-030: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (117467)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-030
Vulnerable Path: C:\windows\system32\rdpudd.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17667

MS16-134: Security Update for Common Log File System Driver (121128)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-134
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18524

MS16-080: Security Update for Microsoft Windows PDF (119492)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-080
Vulnerable Path: C:\windows\system32\glcndfilter.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18336

MS16-048: Security Update for CSRSS (119268)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-048
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18258

MS16-032: Security Update for Secondary Logon to Address Elevation of Privile (119085)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-032
Vulnerable Path: C:\windows\system32\seclogon.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18230

MS16-090: Security Update for Windows Kernel-Mode Drivers (119627)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-090
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18377

MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution (118982)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-014
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18192

MS16-074: Security Update for Microsoft Graphics Component (119498)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-074
Vulnerable Path: C:\windows\system32\gdi32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18344

MS16-060: Security Update for Windows Kernel (119357)

internal | **explicit** | **OS auth**

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-060
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18233

MS18-MAY: Microsoft .NET Security Update (124370)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS18-MAY
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.security.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36440
Remediation KB(s): KB4095876,KB4095517

MS16-073: Security Update for Windows Kernel-Mode Drivers (119499)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-073
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18340

MS17-018: Security Update for Windows Kernel-Mode Drivers (121898)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-018
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18603

MS18-JAN: Microsoft Windows Security Update (MELTDOWN) (123603)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS18-JAN
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18872
Remediation KB(s): KB4056898

MS16-034: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (119083)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-034
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18228

MS16-149: Security Update for Windows (121322)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-149
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS16-135: Security Update for Windows Kernel-Mode Drivers (121127)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-135
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18524

MS16-151: Security Update for Kernel-Mode Driver (121320)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-151
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS16-075: Security Update for Windows SMB Server (119497)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-075
Vulnerable Path: C:\windows\system32\lsasrv.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18298

MS17-017: Security Update for Windows Kernel (121899)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-017
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18603

MS16-018: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (118978)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-018
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18190

MS15-007: Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service (117221)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-007
Vulnerable Path: C:\windows\system32\iassam.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17549

MS16-111: Security Update for Windows Kernel (120911)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-111
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18438

MS17-JUN: Microsoft Internet Explorer Security Update (122280)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-JUN
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18698
Remediation KB(s): KB4021558,KB4022726

MS18-NOV: Microsoft Internet Explorer Security Update (126948)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS18-NOV
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.19180
Remediation KB(s): KB4467697,KB4466536

MS16-008: Security Update for Windows Kernel to Address Elevation of Privilege (118682)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-008
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18185

MS15-015: Vulnerability in Microsoft Windows Could Allow Elevation of Privilege (117375)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-015
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17630

MS15-061: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (117874)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-061
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17837

MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (117582) internal | explicit | OS auth	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS15-038
Vulnerable Path: C:\windows\system32\drivers\clfs.sys
File Version: 6.3.9600.17055
Fixed Version: 6.3.9600.17719

MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (117225) internal | explicit | OS auth	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS15-003
Vulnerable Path: C:\windows\system32\profsvc.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17552

MS15-023: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (117474) internal | explicit | OS auth	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS15-023
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17694

MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (117227) internal | explicit | OS auth	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS15-001
Vulnerable Path: C:\windows\system32\drivers\ahcache.sys
File Version: 6.3.9600.16384
Fixed Version: 6.3.9600.17555

MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution (118662) internal | explicit | OS auth	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS15-132
Vulnerable Path: C:\windows\system32\comsvcs.dll
File Version: 2001.12.10530.17415
Fixed Version: 2001.12.10530.18146

MS15-073: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (118042) internal | explicit | OS auth	N/A / tcp unknown	Medium

Missing Microsoft Patch: MS15-073
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17915

MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (118251)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-102
Vulnerable Path: C:\windows\system32\schedsvc.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18001

MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (118039)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-076
Vulnerable Path: C:\windows\system32\lsasrv.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17918

MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (117730)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-051
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.17796

MS15-072: Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (118043)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-072
Vulnerable Path: C:\windows\system32\gdi32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17902

MS15-119: Security Update for Winsock to Address Elevation of Privilege (118492)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-119
Vulnerable Path: C:\windows\system32\drivers\afd.sys
File Version: 6.3.9600.17194
Fixed Version: 6.3.9600.18089

MS15-133: Security Update for Windows PGM to Address Elevation of Privilege (118661)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-133
Vulnerable Path: C:\windows\system32\drivers\rmcast.sys
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18119

MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege (118128)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-085
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17936

MS15-077: Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (118038)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-077
Vulnerable Path: C:\windows\system32\atmfd.dll
File Version: 5.1.2.238
Fixed Version: 5.1.2.242

MS15-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (117472)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-025
Vulnerable Path: C:\windows\system32\ntoskrnl.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17668

MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege (117731)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-050
Vulnerable Path: C:\windows\system32\services.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17793

MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (119084)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS16-033
Vulnerable Path: C:\windows\system32\drivers\usbstor.sys
File Version: 6.3.9600.17331
Fixed Version: 6.3.9600.18224

MS15-120: Security Update for IPSec to Address Denial of Service (118491)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-120
Vulnerable Path: C:\windows\system32\bfe.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18009

MS16-112: Security Update for Windows Lock Screen (120910)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-112
Vulnerable Path: C:\windows\system32\pnidui.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18434

MS17-016: Security Update for Windows IIS (121900)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-016
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18603

MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass (117223)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-005
Vulnerable Path: C:\windows\system32\nlasvc.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17550

MS16-138: Security Update to Microsoft Virtual Hard Drive (121124)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-138
Vulnerable Path: C:\windows\system32\mshtml.dll
File Version: 11.0.9600.17416
Fixed Version: 11.0.9600.18525

MS15-121: Security Update for Schannel to Address Spoofing (118490)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-121
Vulnerable Path: C:\windows\system32\schannel.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18088

MS19-MAY: Microsoft .NET Security Update (128800)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS19-MAY
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\mscorlib.dll
File Version: 4.0.30319.34014
Fixed Version: 4.0.30319.36543
Remediation KB(s): KB4499408,KB4498963

MS16-153: Security Update for Common Log File System Driver (121318)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-153
Vulnerable Path: C:\windows\system32\win32k.sys
File Version: 6.3.9600.17393
Fixed Version: 6.3.9600.18533

MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service (118975)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS16-021
Vulnerable Path: C:\windows\system32\iassam.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18191

MS17-MAY: Microsoft .NET Security Update (122158)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS17-MAY
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.data.dll
File Version: 4.0.30319.33440
Fixed Version: 4.0.30319.36372
Remediation KB(s): KB4019114

MS15-075: Vulnerabilities in OLE Could Allow Elevation of Privilege (118040)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-075
Vulnerable Path: C:\windows\system32\ole32.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17905

MS15-055: Vulnerability in Schannel Could Allow Information Disclosure (117726)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS15-055
Vulnerable Path: C:\windows\system32\schannel.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17810

MS16-082: Security Update for Microsoft Windows Search Component (119490)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS16-082
Vulnerable Path: C:\windows\system32\structuredquery.dll
File Version: 7.0.9600.17415
Fixed Version: 7.0.9600.18334

MS14-085: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (117082)

N/A / tcp
unknown

Medium

internal | explicit | OS auth

Missing Microsoft Patch: MS14-085
Vulnerable Path: C:\windows\system32\windowscodecs.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17483

MS15-122: Security Update for Kerberos to Address Security Feature Bypass (118489)
internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-122
Vulnerable Path: C:\windows\system32\kerberos.dll
File Version: 6.3.9600.17340
Fixed Version: 6.3.9600.18091

MS16-092: Security Update for Windows Kernel (119625)
internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-092
Vulnerable Path: C:\windows\system32\ntdll.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.18233

MS15-052: Vulnerability in Windows Kernel Could Allow Security Feature Bypass (117729)
internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-052
Vulnerable Path: C:\windows\system32\drivers\cng.sys
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17785

MS15-031: Vulnerability in Schannel Could Allow Security Feature Bypass (117466)
internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-031
Vulnerable Path: C:\windows\system32\schannel.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17702

MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure (118125)
internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-088
Vulnerable Path: C:\windows\system32\notepad.exe
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17930

MS16-065: Security Update for .NET Framework (119353)
internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS16-065
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.dll
File Version: 4.0.30319.34003
Fixed Version: 4.0.30319.34293

MS15-027: Vulnerability in NETLOGON Could Allow Spoofing (117470)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-027
Vulnerable Path: C:\windows\system32\netlogon.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17678

MS17-022: Security Update for Microsoft XML Core Services (121894)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS17-022
Vulnerable Path: C:\windows\system32\msxml3.dll
File Version: 8.110.9600.17415
Fixed Version: 8.110.9600.18574

MS15-016: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (117374)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-016
Vulnerable Path: C:\windows\system32\windowscodecs.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17631

MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure (118129)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-084
Vulnerable Path: C:\windows\system32\msxml3.dll
File Version: 8.110.9600.17415
Fixed Version: 8.110.9600.17931

MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (117468)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-029
Vulnerable Path: C:\windows\system32\wmphoto.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17668

MS15-071: Vulnerability in Netlogon Could Allow Elevation of Privilege (118044)

N/A / tcp
unknown

Medium

internal | **explicit** | **OS auth**

Missing Microsoft Patch: MS15-071
Vulnerable Path: C:\windows\system32\netlogon.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17901

MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass (117376)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-014
Vulnerable Path: C:\windows\system32\scesrv.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17552

MS17-021: Security Update for Windows DirectShow (121895)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS17-021
Vulnerable Path: C:\windows\system32\quartz.dll
File Version: 6.6.9600.17415
Fixed Version: 6.6.9600.18569

MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure (117579)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-041
Vulnerable Path: C:\windows\microsoft.net\framework\v4.0.30319\system.web.dll
File Version: 4.0.30319.34009
Fixed Version: 4.0.30319.34248

MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (117469)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-028
Vulnerable Path: C:\windows\system32\ubpm.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17671

MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass (117222)

internal | explicit | OS auth

N/A / tcp
unknown

Medium

Missing Microsoft Patch: MS15-006
Vulnerable Path: C:\windows\system32\wer.dll
File Version: 6.3.9600.17415
Fixed Version: 6.3.9600.17550

SMB Security Signatures Not Required (104188)

internal | explicit | unauth

139 / tcp
netbios

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

Content Security Policy Missing (148043) **internal | explicit | unauth**	80 / tcp http	Trivial
Missing Content Security Policy.		
Content Security Policy Missing (148043) **internal | explicit | unauth**	8530 / tcp http	Trivial
Missing Content Security Policy.		
Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (120794) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 4 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (120761) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 2 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (120742) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (120631) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120810) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		

Compliance: Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (120760) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (120662) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (120559) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (120756) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings
Result: FAIL

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (120520) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (120616) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (120741) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (120652)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (120646)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (120641)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (120669)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120543)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-271721585-897601226-2024613209-625570482-296978595,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
Result: FAIL

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (120718)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: PASS

Compliance: Configure 'Accounts: Rename administrator account' (120563)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: not Administrator
Collected: Administrator
Result: FAIL

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (120519)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 14
Collected: 0
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120809)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (120715)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (120602)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (120682)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (120574)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (120683)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: C:\Program Files\LAPS\CSE\AdmPwd.dll
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (120737)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (120808)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (120692)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (120754)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (120710)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (120688)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: <= 30
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120554)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-271721585-897601226-2024613209-625570482-296978595,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (120597)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (120762)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (120757)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: *\Internet Explorer\iexplore.exe
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (120530)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (120734) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (120639) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (120687) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: >= 15 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (120790) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (120595) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: 0 Result: PASS		
Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (120593) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (120621) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: 3
Result: FAIL

Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (120661)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (120766)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 196608
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (120648)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (120656)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (120625)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120614)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (120681)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (120717)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (120523)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
Result: FAIL

Compliance: Ensure 'Default Protections for Popular Software' is set to 'Enabled' (120758)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Popular Software
Result: FAIL

Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (120789)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (120575)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Create a token object' is set to 'No One' (120533)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (120814)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (120606)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'EMET 5.5' or higher is installed (120755)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (120585)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (120610)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (120798)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120654)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (120622)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (120788)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (120566)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (120716)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (120712)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120765)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (120799) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (120774) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (120577) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120634) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (120532) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (120714) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (120655)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (120608)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2147483644
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (120677)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (120685)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (120679)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (120551)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (120603)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No Defined Values
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (120815)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (120689)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (120611)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (120544)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (120560)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Prevent the usage of SkyDrive for file storage' is set to 'Enabled' (120792)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (120531)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Link Local Multicast Name Resolution (LLMNR) Enabled (129962)

N/A / tcp
unknown

Trivial

internal | recon | OS auth

LLMNR is enabled

Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (120805)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (120772)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (120817)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Control Panel\Personalization\Force specific screen saver: Screen saver executable name
Result: PASS

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (120591)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (120813)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120644)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (120524)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (120651)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (120587)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (120586)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1 or 2 or 3
Collected: 0
Result: FAIL

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (120619)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Audit Special Logon' is set to 'Success' (120671)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (120568) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (120658) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (120738) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (120736) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (120657) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Audit Security State Change' is set to 'Success' (120678) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (120561) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: 1 Result: FAIL		
Compliance: Ensure 'Deny log on as a service' to include 'Guests' (120539) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: Guests Collected: Empty string Result: FAIL		
Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (120576) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age Result: FAIL		
Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (120612) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: >= 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (120705) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (120822) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
User Configuration\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments Result: PASS		
Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (120592) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (120550)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (120628)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120613)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths and sub-paths' (120601)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

[Large data section omitted]

Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (120607)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (120642)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (120779) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (120694) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120825) N/A / tcp Trivial

internal | compliance | CIS auth unknown

User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges
Result: PASS

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (120713) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (120609) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (120776) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (120629) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

CIS Benchmark Profile (116437)

N/A / tcp
unknown

Trivial

internal | compliance | OS auth

CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0:SERVER

Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (120594)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (120626)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (120541)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (120553)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators,NT SERVICE\\WdiServiceHost
Collected: ADMINISTRATORS,NT SERVICE\WdiServiceHost
Result: PASS

Compliance: Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (120824)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile.
Result: PASS

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (120803) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (120686) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 4 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (120624) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (120572) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (120632) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (120638) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (120618) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (120759)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software
Result: FAIL

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (120516)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 24
Collected: 0
Result: FAIL

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (120795)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120768)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Account Lockout' is set to 'Success' (120667)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (120673)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Profile single process' is set to 'Administrators' (120552) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: Administrators Collected: ADMINISTRATORS Result: PASS		
Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (120650) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (120663) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_SUCCESS Result: FAIL		
Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely... (120690) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 2 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (120630) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (120635) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (120567) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (120819)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Screen saver timeout: Seconds
Result: PASS

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (120700)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: <= 90
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (120670)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Modify an object label' is set to 'No One' (120549)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (120617)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Enable screen saver' is set to 'Enabled' (120816)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver
Result: PASS

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (120811)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (120538)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Password protect the screen saver' is set to 'Enabled' (120818)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Control Panel\Personalization\Password protect the screen saver
Result: PASS

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' (120771)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (120599)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (120623)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (120588)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disa... (120691)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallpublicfw.log' (120653)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: %systemroot%\system32\logfiles\firewall\publicfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (120773)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (120555)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (120675)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (120680)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (120696)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (120751)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallprivatefw.log' (120643)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (120674)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120767)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (120578)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (120582)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (120749)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Shut down the system' is set to 'Administrators' (120556)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (120743)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (120659)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (120525)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Audit Process Creation' is set to 'Success' (120664)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (120589)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (120820)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen
Result: PASS

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120764)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (120562)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (120521)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (120579)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (120697)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: <= 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (120596)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (120615)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

IPv6 Enabled (142306)

N/A / tcp
unknown

Trivial

internal | **explicit** | **OS auth**

IPv6 enabled on network interfaces with the following IPv4 addresses

192.168.67.61

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (120580)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
Result: FAIL

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (120735)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Manage auditing and security log' (120548)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (120784)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120770)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Accounts: Rename guest account' (120564)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: not Guest
Collected: Guest
Result: FAIL

Compliance: Ensure 'Lock pages in memory' is set to 'No One' (120546)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (120528)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,S-1-5-82-271721585-897601226-2024613209-625570482-296978595,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
Result: FAIL

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (120752)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 255
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Logoff' is set to 'Success' (120668)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (120534)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (120637)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (120627)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (120706)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
Result: FAIL

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (120684)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Create symbolic links' (120536)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (120647)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (120800)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (120804)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths' (120600)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Collected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Result: PASS

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (120518)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (120636)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (120649)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (120605)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (120787)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (120704)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (120573)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (120522)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (120645)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (120590)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session
Result: FAIL

Compliance: Ensure 'Deny log on locally' to include 'Guests' (120540)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (120672)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Debug programs' is set to 'Administrators' (120537)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewalldomainfw.log' (120633)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (120753)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (120584)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration
Result: PASS

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (120526) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (120640) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (120517) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
Result: FAIL

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120763) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (120676) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (120581) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120801) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (120783)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (120542)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (120529)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (120535)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (120782)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (120823)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments
Result: PASS

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (120750) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120769) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120807) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (120604) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: 0 Result: PASS		
Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (120545) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: Administrators Collected: ADMINISTRATORS Result: PASS		
Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (120558) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: Administrators Collected: ADMINISTRATORS Result: PASS		
Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120806) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (120565)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (120620)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 2
Collected: 0
Result: FAIL

Default IIS Webpage Detected (117366)
internal | recon | unauth

80 / tcp
http

Trivial

Default IIS Webpage Detected

SMB Native LanMan Version (100092)
internal | recon | unauth

139 / tcp
netbios

Trivial

LAN Manager: 6.3.9600.15
Domain: WIN-30QQRC10MGG
OS: Windows 2012 R2 Build 9600

Asset Comments and Notes

Comment | Jasmine Zaker (jasmine.zaker@helpsystems.com) | Monday, Aug. 15, 2022 12:39 PM CDT
example note for remediation 123

WIN-30QQRC10MGG D

IP: 192.168.68.107
Asset name: WIN-30QQRC10MGG
Operating system: Windows Server 2012 R2
Asset type: Server

Protocol	Service
http	80 / tcp
msrpc	135 / tcp

netbios	139 / tcp
smb	445 / tcp
lpd	515 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) (117590) **internal** | **explicit** | **unauth**	80 / tcp http	High
[Large data section omitted]		
MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756) **internal** | **explicit** | **unauth**	135 / tcp msrpc	Medium
This asset permits binding to samr pipe using auth level Connect. Response from asset: 02 . 22 00 00 c0 "... Responding port: 49153		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Low

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Connection: Sweet32 Vulnerability (121110)

3389 / tcp
msrdp

Trivial

internal | explicit | unauth

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.2:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

3389 / tcp
msrdp

Trivial

internal | explicit | unauth

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

3389 / tcp
msrdp

Trivial

internal | explicit | unauth

Weak Signature Algorithm: SHA-1

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

3389 / tcp
msrdp

Trivial

internal | explicit | unauth

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: ECDHE-RSA-AES256-SHA

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (120572)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (120631)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (120630)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (120790)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (120595)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120613)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Deny log on as a service' to include 'Guests' (120539)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (120716) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (120799) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (120638) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (120520) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 0 Result: FAIL		
Compliance: Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (120824) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile. Result: FAIL		
Compliance: Ensure 'Audit Special Logon' is set to 'Success' (120671) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS Collected: AUDIT_SUCCESS Result: PASS		
Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (120754) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (120714)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (120623)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (120773)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Accounts: Rename administrator account' (120563)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: not Administrator
Collected: Administrator
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120825)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges
Result: FAIL

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (120558)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (120525) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (120794) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (120521) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (120715) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120644) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120770) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (120615) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Configure 'Accounts: Rename guest account' (120564)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: not Guest
Collected: Guest
Result: FAIL

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (120663)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (120632)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (120594)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (120648)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (120672)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (120576) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age
Result: FAIL

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (120577) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (120674) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (120582) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (120578) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120543) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (120645) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (120528)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
Result: FAIL

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (120706)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
Result: FAIL

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (120610)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (120640)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (120642)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (120519)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 14
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (120629)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (120516)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 24
Collected: 0
Result: FAIL

Compliance: Ensure 'Lock pages in memory' is set to 'No One' (120546)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Shut down the system' is set to 'Administrators' (120556)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (120686)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent the usage of SkyDrive for file storage' is set to 'Enabled' (120792)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Modify an object label' is set to 'No One' (120549)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (120639)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (120649)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (120611)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (120655)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (120782)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (120795)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120809)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (120817)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Control Panel\Personalization\Force specific screen saver: Screen saver executable name
Result: FAIL

Compliance: Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (120822)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments
Result: FAIL

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (120776)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (120811)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (120680)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120767)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (120673)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120801)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (120529)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (120618)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (120800)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (120738)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (120804)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (120783)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password protect the screen saver' is set to 'Enabled' (120818)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Control Panel\Personalization\Password protect the screen saver
Result: FAIL

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (120675)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (120608)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2147483644
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (120687)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (120766)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 196608
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (120808) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (120717) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (120544) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120806) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable screen saver' is set to 'Enabled' (120816) N/A / tcp unknown Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120807) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (120789) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (120628) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (120530) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: Administrators,LOCAL SERVICE Collected: LOCAL SERVICE,ADMINISTRATORS Result: PASS		
Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (120736) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120654) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: >= 16384 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (120662) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_SUCCESS Result: FAIL		
Compliance: Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (120760) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (120677) N/A / tcp Trivial
internal | **compliance** | **CIS auth** unknown

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (120617) N/A / tcp Trivial
internal | **compliance** | **CIS auth** unknown

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (120619) N/A / tcp Trivial
internal | **compliance** | **CIS auth** unknown

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (120531) N/A / tcp Trivial
internal | **compliance** | **CIS auth** unknown

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (120635) N/A / tcp Trivial
internal | **compliance** | **CIS auth** unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (120713) N/A / tcp Trivial
internal | **compliance** | **CIS auth** unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (120626)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120554)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
Result: FAIL

Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (120712)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (120753)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (120656)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (120622)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (120588)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (120522)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (120573)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (120803)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (120621)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 3
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (120641)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (120590)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session
Result: FAIL

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120768) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (120784) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120810) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (120589) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (120787) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (120694) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (120599) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Audit Logoff' is set to 'Success' (120668) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Configure 'Create symbolic links' (120536) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (120609) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (120602) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (120741) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (120704) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (120650) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths and sub-paths' (120601)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

[Large data section omitted]

Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (120604)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (120606)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (120551)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (120788)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (120587)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (120688)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 30
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (120591)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (120560)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (120658)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (120814)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (120737)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (120534)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (120566)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (120819)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Control Panel\Personalization\Screen saver timeout: Seconds
Result: FAIL

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (120734)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (120575)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (120555)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (120524)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (120518)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (120584)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration
Result: PASS

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (120779)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on locally' to include 'Guests' (120540)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (120696)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Process Creation' is set to 'Success' (120664)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (120683)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: C:\Program Files\LAPS\CSE\AdmPwd.dll
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' (120771)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (120580)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
Result: FAIL

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (120676)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (120820)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen
Result: FAIL

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (120535)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (120532)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (120620)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (120646)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (120798)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (120805)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (120565)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Account Lockout' is set to 'Success' (120667)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (120813)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Debug programs' is set to 'Administrators' (120537) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Network access: Remotely accessible registry paths' (120600) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Collected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (120636) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120634) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (120700) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: <= 90
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (120597) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (120710)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (120756)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings
Result: FAIL

Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (120685)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (120517)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
Result: FAIL

Compliance: Ensure 'Create a token object' is set to 'No One' (120533)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (120567)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (120607)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (120735)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Protections for Popular Software' is set to 'Enabled' (120758)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Popular Software
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (120579)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (120689)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (120625)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (120762)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (120605)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (120553)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators,NT SERVICE\\WdiServiceHost
Collected: ADMINISTRATORS,NT SERVICE\WdiServiceHost
Result: PASS

Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (120581)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (120561)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewalldomainfw.log' (120633)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (120679)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (120743)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (120750)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (120612)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: 1
Result: PASS

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (120550)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (120759)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software
Result: FAIL

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (120692)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (120815)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (120585) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (120603) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: No Defined Values
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (120669) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (120772) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120763) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (120742) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (120684)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallpublicfw.log' (120653)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: %systemroot%\system32\logfiles\firewall\publicfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (120627)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (120545)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (120661)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (120538)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (120526)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (120652)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (120562)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (120523)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
Result: FAIL

Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (120593)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (120682)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120769)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Manage auditing and security log' (120548)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (120697)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (120596)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (120823)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallprivatefw.log' (120643)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (120637)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (120670)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (120761)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (120542)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disa... (120691)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120614)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (120559)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (120541)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (120657)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120764)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security State Change' is set to 'Success' (120678)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely... (120690)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (120681)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (120718)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: PASS

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (120752)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 255
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (120651)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'EMET 5.5' or higher is installed (120755)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (120586)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1 or 2 or 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (120705)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (120774)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (120757)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: *\Internet Explorer\iexplore.exe
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (120751)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (120616)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (120574)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (120624)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (120749)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (120592)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (120659)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120765) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (120647) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Profile single process' is set to 'Administrators' (120552) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (120568) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

TLS Connection: TLS Version 1.0 Enabled (125641) 3389 / tcp msrdp Trivial

internal | explicit | unauth

Server supports TLS version 1.0

SMB Native LanMan Version (100092) 139 / tcp netbios Trivial

internal | recon | unauth

LAN Manager: 6.3.9600.15
Domain: WIN-30QQRC10MGG
OS: Windows 2012 R2 Build 9600

NTLM Authentication Host Information Disclosure (117943) 80 / tcp http Trivial

internal | recon | unauth

NetBIOS Domain: WIN-30QQRC10MGG
NetBIOS Hostname: WIN-30QQRC10MGG
DNS Domain Name: WIN-30QQRC10MGG
DNS Hostname: WIN-30QQRC10MGG

Default IIS Webpage Detected (117366) **internal | recon | unauth**	80 / tcp http	Trivial

Default IIS Webpage Detected

192.168.68.151 D

IP: 192.168.68.151
Asset name: 192.168.68.151
Operating system: Windows 7
Asset type: Client

Protocol	Service
ssh	22 / tcp
unknown	139 / tcp
vnc	5900 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Microsoft Windows 7 End of Life (131864) **internal | explicit | unauth**	N/A / tcp unknown	High

Support has ended for Windows 7. This host should be immediately upgraded.

SMB Native LanMan Version (100092) **internal | recon | unauth**	139 / tcp unknown	Trivial

LAN Manager: 6.1.7600.0
Domain: MBP-MAC
OS: Windows 7 Build 7600

WIN-30QQRC10MGG D

IP: 192.168.69.104

Asset name: WIN-30QQRC10MGG
Operating system: Windows Server 2012 R2
Asset type: Server

Protocol	Service
http	80 / tcp
msrpc	135 / tcp
netbios	139 / tcp
smb	445 / tcp
lpd	515 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) (117590) **internal** | **explicit** | **unauth**	80 / tcp http	High
[Large data section omitted]		
MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756) **internal** | **explicit** | **unauth**	135 / tcp msrpc	Medium

This asset permits binding to samr pipe using auth level Connect.
Response from asset:
02 .

22 00 00 c0 "...

Responding port: 49153

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

3389 / tcp
msrdp

Low

internal | **explicit** | **unauth**

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Connection: Sweet32 Vulnerability (121110)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

Weak Signature Algorithm: SHA-1

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: ECDHE-RSA-AES256-SHA

Compliance: Ensure 'Enable screen saver' is set to 'Enabled' (120816) N/A / tcp Trivial
unknown
internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver
Result: PASS

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (120784) N/A / tcp Trivial
unknown
internal | **compliance** | **CIS auth**

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (120612) N/A / tcp Trivial
unknown
internal | **compliance** | **CIS auth**

Expected: >= 1
Collected: 1
Result: PASS

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (120625) N/A / tcp Trivial
unknown
internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (120808) N/A / tcp Trivial
unknown
internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (120694) N/A / tcp Trivial
unknown
internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (120640) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (120621) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 3
Result: FAIL

Compliance: Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (120817) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Force specific screen saver: Screen saver executable name
Result: PASS

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (120682) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (120706) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120613) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (120594)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (120689)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (120736)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (120530)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (120685)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (120752)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 255
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (120529)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120764)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120554)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-271721585-897601226-2024613209-625570482-296978595,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
Result: FAIL

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (120700)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: <= 90
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (120622)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (120608)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2147483644
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (120713)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (120783)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (120823)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments
Result: PASS

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120768)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (120534)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120644)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (120705)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (120595)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (120756)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings
Result: FAIL

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (120675)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (120581)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Shut down the system' is set to 'Administrators' (120556)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (120741)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (120593)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (120674)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (120735)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (120716)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (120572)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (120677)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120763)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (120579)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (120645)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (120580)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
Result: FAIL

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (120541)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120654)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (120609)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Prevent the usage of SkyDrive for file storage' is set to 'Enabled' (120792) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (120761) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 2 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'EMET 5.5' or higher is installed (120755) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 2 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (120574) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (120776) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120806) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (120814) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		

Compliance: Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (120759)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software
Result: FAIL

Compliance: Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (120820)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen
Result: PASS

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (120737)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Process Creation' is set to 'Success' (120664)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (120638)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (120624)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Password protect the screen saver' is set to 'Enabled' (120818)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Control Panel\Personalization\Password protect the screen saver
Result: PASS

Compliance: Ensure 'Default Protections for Popular Software' is set to 'Enabled' (120758) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Popular Software
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120807) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (120616) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120801) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (120779) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Debug programs' is set to 'Administrators' (120537) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120809) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (120589)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (120655)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (120518)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (120651)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (120798)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (120641)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (120519)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 14
Collected: 0
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (120587)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (120531)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Modify an object label' is set to 'No One' (120549)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (120766)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 196608
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewalldomainfw.log' (120633)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (120649)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (120648)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (120663)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (120577)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Lock pages in memory' is set to 'No One' (120546)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (120585)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (120683)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: C:\Program Files\LAPS\CSE\AdmPwd.dll
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (120718) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (120637) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (120734) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (120610) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (120684) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (120804) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (120586) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1 or 2 or 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120767) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (120704) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely... (120690) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (120538) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (120790) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (120639)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (120692)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (120575)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (120799)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (120642)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120770)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120614)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (120757)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: *\Internet Explorer\iexplore.exe
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (120573)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (120749)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (120551)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (120526)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (120805)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (120620)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2
Collected: 0
Result: FAIL

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (120567)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (120520)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths and sub-paths' (120601)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

[Large data section omitted]

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (120578)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (120631)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Account Lockout' is set to 'Success' (120667)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (120566)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (120822)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments
Result: PASS

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (120794)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (120662)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Configure 'Create symbolic links' (120536)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (120772)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (120582)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (120795)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (120522)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (120824)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile.
Result: PASS

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (120803)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (120603)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: No Defined Values
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (120627)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (120525) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (120774) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (120588) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (120762) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (120623) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (120561) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (120773)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on locally' to include 'Guests' (120540)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (120599)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disa... (120691)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (120528)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,S-1-5-82-271721585-897601226-2024613209-625570482-296978595,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
Result: FAIL

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (120576)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age
Result: FAIL

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (120751) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (120743) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (120679) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (120815) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (120607) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (120647) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120769) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (120819)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Control Panel\Personalization\Screen saver timeout: Seconds
Result: PASS

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (120532)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (120604)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (120738)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (120789)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallprivatefw.log' (120643)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (120629)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (120617)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (120696)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (120672)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (120521)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (120560)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 3
Collected: 0
Result: FAIL

Compliance: Configure 'Accounts: Rename administrator account' (120563)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: not Administrator
Collected: Administrator
Result: FAIL

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (120670)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (120558)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (120813)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (120754)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (120714)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (120800)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (120517) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
Result: FAIL

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (120524) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (120523) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (120592) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallpublicfw.log' (120653) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: %systemroot%\system32\logfiles\firewall\publicfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (120811) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (120602) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120543)
N/A / tcp
unknown
Trivial

internal | **compliance** | **CIS auth**

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-271721585-897601226-2024613209-625570482-296978595,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415,S-1-5-82-3876422241-1344743610-1729199087-774402673-2621913236
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (120591)
N/A / tcp
unknown
Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (120630)
N/A / tcp
unknown
Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (120562)
N/A / tcp
unknown
Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (120542)
N/A / tcp
unknown
Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (120628)
N/A / tcp
unknown
Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (120555) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (120618) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (120646) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (120715) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (120516) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: >= 24
Collected: 0
Result: FAIL

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (120788) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (120661) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (120697) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: <= 5 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Logoff' is set to 'Success' (120668) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS Collected: AUDIT_SUCCESS Result: PASS		
Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120765) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (120688) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: <= 30 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (120597) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 0 Result: FAIL		
Compliance: Ensure 'Audit Special Logon' is set to 'Success' (120671) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS Collected: AUDIT_SUCCESS Result: PASS		

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (120544) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (120669) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Network access: Remotely accessible registry paths' (120600) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Collected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Result: PASS

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120825) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges
Result: PASS

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (120590) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session
Result: FAIL

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (120710) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (120676)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (120550)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (120632)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (120545)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (120681)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (120680)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Create a token object' is set to 'No One' (120533)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (120596)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (120553)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators,NT SERVICE\\WdiServiceHost
Collected: ADMINISTRATORS,NT SERVICE\WdiServiceHost
Result: PASS

Compliance: Ensure 'Audit Security State Change' is set to 'Success' (120678)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (120657)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (120656)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (120658)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (120652)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (120659)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (120717)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (120565)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (120635)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Manage auditing and security log' (120548)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (120712)

internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (120611)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120634)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (120753)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (120782)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (120605)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (120673)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (120626)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (120559)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (120742)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (120606)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (120615)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (120760)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (120750)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a service' to include 'Guests' (120539)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (120619)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Configure 'Accounts: Rename guest account' (120564)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: not Guest
Collected: Guest
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (120636)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (120686)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (120535)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' (120771)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (120568)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (120787)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120810)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (120687)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (120584)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration
Result: PASS

Compliance: Ensure 'Profile single process' is set to 'Administrators' (120552)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (120650) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

NTLM Authentication Host Information Disclosure (117943) internal | recon | unauth	80 / tcp http	Trivial

NetBIOS Domain: WIN-30QQRC10MGG
NetBIOS Hostname: WIN-30QQRC10MGG
DNS Domain Name: WIN-30QQRC10MGG
DNS Hostname: WIN-30QQRC10MGG

Default IIS Webpage Detected (117366) internal | recon | unauth	80 / tcp http	Trivial

Default IIS Webpage Detected

SMB Native LanMan Version (100092) internal | recon | unauth	139 / tcp netbios	Trivial

LAN Manager: 6.3.9600.15
Domain: WIN-30QQRC10MGG
OS: Windows 2012 R2 Build 9600

TLS Connection: TLS Version 1.0 Enabled (125641) internal | explicit | unauth	3389 / tcp msrdp	Trivial

Server supports TLS version 1.0

192.168.69.140 D

IP: 192.168.69.140
Asset name: 192.168.69.140
Operating system: Windows 7
Asset type: Client

Protocol	Service
ssh	22 / tcp
unknown	139 / tcp
vnc	5900 / tcp

unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Microsoft Windows 7 End of Life (131864) **internal | explicit | unauth**	N/A / tcp unknown	High
Support has ended for Windows 7. This host should be immediately upgraded.		
SMB Native LanMan Version (100092) **internal | recon | unauth**	139 / tcp unknown	Trivial
LAN Manager: 6.1.7600.0 Domain: MBP-MAC OS: Windows 7 Build 7600		

BRW105BAD6F7090 D

IP: 192.168.86.37
Asset name: BRW105BAD6F7090
Operating system: Brother NC Printer
Asset type: Printer

Protocol	Service
http	80 / tcp
netbios-ns	137 / udp
snmp	161 / udp
http (ssl)	443 / tcp
pjl	9100 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SNMP Writeable Communities (104067) **internal** | **explicit** | **unauth**	161 / udp snmp	High
internal		
SNMP Default Communities (100149) **internal** | **explicit** | **unauth**	161 / udp snmp	Medium
internal public		

10.1.1.21 C

IP: 10.1.1.21
Asset name: 10.1.1.21
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
rpcbind	111 / tcp
rpcbind	111 / udp
msrdp	3389 / tcp
postgresql (ssl)	5432 / tcp
mountd	36657 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

OpenSSH Account Enumeration Vulnerability (126640)
internal | potential | unauth

22 / tcp
ssh

Medium

8.9p1

RPC Portmap Service (100505)
internal | explicit | unauth

111 / udp
rpcbind

Trivial

Not Applicable

RPC Portmap Service (100505)
internal | explicit | unauth

111 / tcp
rpcbind

Trivial

Not Applicable

Remote Desktop Protocol Allows Man in the Middle (117858)
internal | explicit | unauth

3389 / tcp
msrdp

Trivial

rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)

TLS Connection: TLS Version 1.2 Not Enabled (146258)
internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server does not support TLS version 1.2

MSSQL-SERVER C

IP: 192.168.0.106
Asset name: MSSQL-SERVER
Operating system: Windows Server 2016
Asset type: Server

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
tds	1433 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp

unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
NetBIOS Shares Accessible (100870) **internal | explicit | unauth**	139 / tcp netbios	Medium
NetBIOS Accessible Shares: Users (READ)		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	1433 / tcp tds	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.1 RC4-MD5 - TLSv1.2 RC4-SHA - TLSv1.2		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.1 RC4-MD5 - TLSv1.2 RC4-SHA - TLSv1.2		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp netbios	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

1433 / tcp
tds

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

1433 / tcp
tds

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

1433 / tcp
tds

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SMB Native LanMan Version (100092) 139 / tcp Trivial
internal | recon | unauth netbios

LAN Manager: 10.0.14393.15
Domain: ISMAILDOMAIN
OS: Windows 2016 Build 14393

TLS Connection: TLS Version 1.0 Enabled (125641) 3389 / tcp Trivial
internal | explicit | unauth msrdp

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) 3389 / tcp Trivial
internal | explicit | unauth msrdp

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641) 1433 / tcp Trivial
internal | explicit | unauth tds

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) 1433 / tcp Trivial
internal | explicit | unauth tds

Server supports TLS version 1.1

TDS SQL Database Service (101436) 1433 / tcp Trivial
internal | recon | unauth tds

TDS SQL database service detected

HPC41F34 C

IP: 192.168.0.150
Asset name: HPC41F34
Operating system: unknown
Asset type: Printer

Protocol	Service
http	80 / tcp

netbios-ns	137 / udp
snmp	161 / udp
http (ssl)	443 / tcp
http	631 / tcp
http	8080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SNMP Default Communities (100149) **internal | explicit | unauth**	161 / udp snmp	Medium
internal public		
Protocol Allows Authentication Over Clear Text (104798) **internal | explicit | unauth**	161 / udp snmp	Low
snmp allows transmission of credentials in clear text		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
SSL connection supports the following SSLv3/TLSv1 CBC mode cipher: AES128-SHA - TLSv1 AES256-SHA - TLSv1 DHE-RSA-AES128-SHA - TLSv1 DHE-RSA-AES256-SHA - TLSv1 BEAST not mitigated: all supported ciphers are CBC mode ciphers		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Server supports TLS version 1.1		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial

	Server supports TLS version 1.0

HTORRES1018	**C**

IP: 192.168.0.191
Asset name: HTORRES1018
Operating system: Windows 10 Enterprise
Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
http (ssl)	443 / tcp
vmwareauth	902 / tcp
vmwareauth	912 / tcp
msrdp	3389 / tcp
http	5700 / tcp
general	N/A / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	Failure	N/A	Failure	Failure

Vulnerability Title	Service(s)	Severity
MS17-JUN: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128597) **internal | explicit | OS auth**	N/A / tcp general	Medium

MS17-JUN: Microsoft Internet Explorer Security Update is installed but the registry entry has not been set.

Registry keys missing:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1

MS17-SEP: Microsoft Internet Explorer Security Update - Registry Entry Not Set (128598)

internal | explicit | OS auth

N/A / tcp
general

Medium

MS17-SEP: Microsoft Internet Explorer Security Update is installed but the registry entry has not been set.

Registry keys missing:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet
Explorer\MAIN\FeatureControl\FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX\iexplore.exe => 1

Zoom 'Share Screen' Information Disclosure Vulnerability (144747)

internal | explicit | OS auth

N/A / tcp
general

Medium

Version: 5.2.42619.804
Path: \users\hernan.torres\appdata\roaming\zoom\bin\zoom.exe

SMB Security Signatures Not Required (104188)

internal | explicit | unauth

139 / tcp
netbios

Low

SMBv2 NTLM signatures are not required

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

SMB Native LanMan Version (100092)

internal | **recon** | **unauth**

139 / tcp
netbios

Trivial

LAN Manager: 10.0.19041.15
Domain: HELPSYSTEMS
OS: Windows 10 Build 19041

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.1

SSL Certificate: Expired Certificate Date (103615)

internal | **explicit** | **unauth**

902 / tcp
vmwareauth

Trivial

Date Appears Invalid: Feb 4 12:50:53 2021 GMT to Feb 4 12:50:53 2022 GMT

SSL Certificate: Expired Certificate Date (103615)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Trivial

Date Appears Invalid: Feb 4 12:50:53 2021 GMT to Feb 4 12:50:53 2022 GMT

IPv6 Enabled (142306)

internal | **explicit** | **OS auth**

N/A / tcp
general

Trivial

IPv6 enabled on network interfaces with the following IPv4 addresses
192.168.56.1
192.168.1.1
192.168.253.1
172.30.208.1
192.168.95.1
192.168.1.49

NetBIOS Over TCP/IP Enabled (124295)

internal | **recon** | **OS auth**

N/A / tcp
general

Trivial

```
NetBIOS is enabled:
GUID: {0a4f9943-0787-4de7-86cd-b0e77fe3742f} - Value: 0
GUID: {3243b081-aafc-43d0-8ad5-29f8b883a877} - Value: 0
GUID: {392a1a5a-9fb2-4f63-b9e3-6801e305ecef} - Value: 0
GUID: {873066ef-35ae-4540-ab5f-691cbd02cd36} - Value: 0
GUID: {876cd0fa-3f5b-4dff-a9c8-ad5742720a07} - Value: 0
GUID: {e0dda76d-b1bb-451a-862f-3900f32dc752} - Value: 0
```

192.168.1.60 C

IP: 192.168.1.60
Asset name: 192.168.1.60
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
http (ssl)	443 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
jQuery Cross-Site Scripting Vulnerability (144402) **internal | potential | unauth**	80 / tcp http	Medium
1.11.3		
jQuery Ajax Cross-Site Scripting Vulnerability (126532) **internal | potential | unauth**	80 / tcp http	Medium
1.11.3		
jQuery Cross-Site Scripting Vulnerability (137374) **internal | potential | unauth**	80 / tcp http	Medium
1.11.3		

jQuery Cross-Site Scripting Vulnerability (144402) **internal | potential | unauth**	443 / tcp http (ssl)	Medium
1.11.3		
jQuery Ajax Cross-Site Scripting Vulnerability (126532) **internal | potential | unauth**	443 / tcp http (ssl)	Medium
1.11.3		
jQuery Cross-Site Scripting Vulnerability (137374) **internal | potential | unauth**	443 / tcp http (ssl)	Medium
1.11.3		
OpenSSH Account Enumeration Vulnerability (126640) **internal | potential | unauth**	22 / tcp ssh	Medium
Not Applicable		
Web Server Directory Indexing Enabled (101049) **internal | explicit | unauth**	80 / tcp http	Low
Directory Indexing Enabled: 192.168.1.60:80: /css /images /images/br /images/de /images/fake /js		
Web Server Directory Indexing Enabled (101049) **internal | explicit | unauth**	443 / tcp http (ssl)	Low
Directory Indexing Enabled: 192.168.1.60:443: /css /images /images/br /images/de /images/fake /js		

WIN-30QQRC10MGG C

IP: 192.168.68.104
Asset name: WIN-30QQRC10MGG
Operating system: Windows Server 2012 R2
Asset type: Server

Protocol	Service

http	80 / tcp
http	83 / tcp
msrpc	135 / tcp
netbios	139 / tcp
http (ssl)	443 / tcp
smb	445 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
unknown (ssl)	8443 / tcp
http	9999 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756) **internal | explicit | unauth**	135 / tcp msrpc	Medium
This asset permits binding to samr pipe using auth level Connect. Response from asset: 02 . 22 00 00 c0 "... Responding port: 49156		
Insecure Crossdomain.xml Directives (104181) **internal | explicit | unauth**	83 / tcp http	Low

```
Path: /crossdomain.xml
Content:
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
<allow-access-from domain="*" />
</cross-domain-policy>
```

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

3389 / tcp
msrdp

Low

internal | **explicit** | **unauth**

```
Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2
```

SSL Connection: Sweet32 Vulnerability (121110)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

```
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.2:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA
```

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

```
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2
```

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

```
Weak Signature Algorithm: SHA-1
```

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: ECDHE-RSA-AES256-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Certificate: Outdated Version (104020)

internal | **explicit** | **unauth**

8443 / tcp
unknown (ssl)

Trivial

Outdated SSL Certificate Version: 1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

SMB Native LanMan Version (100092)

internal | **recon** | **unauth**

139 / tcp
netbios

Trivial

LAN Manager: 6.3.9600.15
Domain: WIN-30QQRC10MGG
OS: Windows 2012 R2 Build 9600

SSL Certificate: Outdated Version (104020)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Trivial

Outdated SSL Certificate Version: 1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | **explicit** | **unauth**

443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.0

Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (120754)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Accounts: Rename administrator account' (120563)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: not Administrator
Collected: Administrator
Result: FAIL

Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120543)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
Result: FAIL

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (120562)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallpublicfw.log' (120653)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: %systemroot%\system32\logfiles\firewall\publicfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (120592)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (120517)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
Result: FAIL

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (120602)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (120688)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: <= 30
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (120676)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (120590)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session
Result: FAIL

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (120736)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (120784)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (120808)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (120687) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (120622) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120768) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (120737) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (120820) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewalldomainfw.log' (120633) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (120766)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 196608
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (120531)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Modify an object label' is set to 'No One' (120549)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (120587)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (120519)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 14
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (120641)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (120798)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (120651) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Debug programs' is set to 'Administrators' (120537) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (120779) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120801) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (120655) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (120518) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: >= 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (120589)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (120586)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1 or 2 or 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (120804)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (120684)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (120610)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (120734)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (120637)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (120639)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (120790)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (120538)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120767)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (120663)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (120649)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (120648)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (120718)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: PASS

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (120683)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: C:\Program Files\LAPS\CSE\AdmPwd.dll
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (120585)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Lock pages in memory' is set to 'No One' (120546)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (120577)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (120551)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (120749) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (120573) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (120757) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: *\Internet Explorer\iexplore.exe
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120614) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths and sub-paths' (120601) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

[Large data section omitted]

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (120520) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (120620) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 2 Collected: 0 Result: FAIL		
Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (120805) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (120692) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: 1 Result: FAIL		
Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (120584) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration Result: PASS		
Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (120795) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (120627) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (120603) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: No Defined Values
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (120803) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (120824) N/A / tcp unknown Trivial

internal | compliance | CIS auth

User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile.
Result: FAIL

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (120522) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (120566) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (120631) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (120582) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Configure 'Create symbolic links' (120536)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (120794)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (120662)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (120822)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments
Result: FAIL

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (120751)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (120743)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (120576)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age
Result: FAIL

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (120599)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Deny log on locally' to include 'Guests' (120540)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (120815)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (120679)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (120774)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (120525)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (120650)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (120773)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (120762)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (120623)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (120819)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Screen saver timeout: Seconds
Result: FAIL

Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (120604)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (120532) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: Administrators Collected: ADMINISTRATORS Result: PASS		
Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (120647) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (120607) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (120670) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_NONE Result: FAIL		
Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (120681) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (120550) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: Administrators Collected: ADMINISTRATORS Result: PASS		
Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (120545) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (120553)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,NT SERVICE\\WdiServiceHost
Collected: ADMINISTRATORS,NT SERVICE\WdiServiceHost
Result: PASS

Compliance: Ensure 'Create a token object' is set to 'No One' (120533)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (120626)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (120561)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Configure 'Manage auditing and security log' (120548)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (120706)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
Result: FAIL

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (120682)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (120817)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Control Panel\Personalization\Force specific screen saver: Screen saver executable name
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (120621)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 3
Result: FAIL

Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (120594)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (120689)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120613)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (120612)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: 1
Result: PASS

Compliance: Ensure 'Enable screen saver' is set to 'Enabled' (120816)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (120640)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (120800)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (120714)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (120560)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (120521)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (120672)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (120696)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (120617)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (120789)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallprivatefw.log' (120643)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (120591)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (120523)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
Result: FAIL

Compliance: Ensure 'Audit Special Logon' is set to 'Success' (120671)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120825)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths' (120600)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Collected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (120646)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (120628)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (120516) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: >= 24 Collected: 0 Result: FAIL		
Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (120659) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_SUCCESS Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (120632) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (120606) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (120742) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (120760) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 3 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120634) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (120635)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (120753)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' (120771)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120810)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (120787)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a service' to include 'Guests' (120539)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (120750) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (120535) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (120686) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Accounts: Rename guest account' (120564) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: not Guest
Collected: Guest
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (120636) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (120619) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (120694)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (120625)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (120713)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (120608)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2147483644
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120644)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (120534)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (120823)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments
Result: FAIL

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (120783)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (120529)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (120752)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 255
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (120530)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (120700)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: <= 90
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120554)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
Result: FAIL

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120764)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (120579)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120763)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent the usage of SkyDrive for file storage' is set to 'Enabled' (120792)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (120609)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (120541)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120654)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (120580)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (120645)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (120674)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (120593)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (120741)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Shut down the system' is set to 'Administrators' (120556)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (120581)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (120675)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (120756)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings
Result: FAIL

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (120595)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (120705)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (120677)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (120572)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (120716)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (120735)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password protect the screen saver' is set to 'Enabled' (120818)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Password protect the screen saver
Result: FAIL

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (120624)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Process Creation' is set to 'Success' (120664)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (120638)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120807) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Protections for Popular Software' is set to 'Enabled' (120758) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Popular Software
Result: FAIL

Compliance: Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (120759) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (120814) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120806) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (120574) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'EMET 5.5' or higher is installed (120755) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (120761) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120809) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (120616) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely... (120690) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (120704) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120770) N/A / tcp Trivial
internal | compliance | CIS auth unknown

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (120642)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (120567)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (120526)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (120799)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (120575)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (120776)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Account Lockout' is set to 'Success' (120667)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (120578) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (120772) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disa... (120691) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (120528) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
Result: FAIL

Compliance: Ensure 'Profile single process' is set to 'Administrators' (120552) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (120588) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (120738) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120769) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (120558) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (120813) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (120629) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (120542) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (120630) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (120524) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (120811) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (120597) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120765) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (120710) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (120669) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (120544)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (120715)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (120618)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (120555)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Audit Logoff' is set to 'Success' (120668)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (120697)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (120661)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (120788)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (120658)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (120652)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (120656)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (120657)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Audit Security State Change' is set to 'Success' (120678)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (120565)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (120717)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (120596)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (120680)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (120559)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (120615)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (120712)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (120673) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (120605) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (120782) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (120568) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (120611) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (120685) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

WIN-30QQRC10MGG **C**

IP: 192.168.69.132
Asset name: WIN-30QQRC10MGG
Operating system: Windows Server 2012 R2
Asset type: Server

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
smb	445 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756) **internal** | **explicit** | **unauth**	135 / tcp msrpc	Medium

```
This asset permits binding to samr pipe using auth level Connect.
Response from asset:
02 .

22 00 00 c0 "...

Responding port: 49154
```

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Low

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SMB Security Signatures Not Required (104188)

internal | **explicit** | **unauth**

139 / tcp
netbios

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

SSL Connection: Sweet32 Vulnerability (121110)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: ECDHE-RSA-AES256-SHA

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (120623)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (120523)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold
Result: FAIL

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (120617)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (120779)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (120567)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (120805)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (120774)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (120535)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (120639)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (120638)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr' (120817)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Control Panel\Personalization\Force specific screen saver: Screen saver executable name
Result: PASS

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (120790)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (120682) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (120528) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (120637) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120806) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (120772) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (120706) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (120814) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (120631) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (120679) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'System DEP' is set to 'Enabled: Application Opt-Out' (120761) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (120625) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (120629) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (120559) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (120672) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120554) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE
Result: PASS

Compliance: Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0' (120819) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

User Configuration\Administrative Templates\Control Panel\Personalization\Screen saver timeout: Seconds
Result: PASS

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (120521) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120769) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (120582) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: Any text
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled' (120820) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

User Configuration\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen
Result: PASS

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (120524) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (120551) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (120776) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (120655) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (120736) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (120658) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (120809) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallprivatefw.log' (120643) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (120620) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 2
Collected: 0
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (120717) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (120783) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (120773) N/A / tcp Trivial

internal | compliance | CIS auth unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (120628)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (120787)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (120704)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create a token object' is set to 'No One' (120533)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (120641)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (120607)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (120713)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (120616) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (120687) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (120754) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (120647) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (120751) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120825) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges
Result: PASS

Compliance: Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings) (120756)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings
Result: FAIL

Compliance: Ensure 'Debug programs' is set to 'Administrators' (120537)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Deny log on as a service' to include 'Guests' (120539)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (120735)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (120663)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (120592)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled' (120822)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments
Result: PASS

Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (120545)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120767)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (120657)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (120585)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Password protect the screen saver' is set to 'Enabled' (120818)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

User Configuration\Administrative Templates\Control Panel\Personalization\Password protect the screen saver
Result: PASS

Compliance: Ensure 'Network access: Remotely accessible registry paths and sub-paths' (120601)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

[Large data section omitted]

Compliance: Ensure 'Audit Special Logon' is set to 'Success' (120671)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (120578) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (120635) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (120518) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: >= 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (120753) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (120642) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (120589) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (120610) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Configure 'Create symbolic links' (120536) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewalldomainfw.log' (120633) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (120597) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (120553) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators,NT SERVICE\\WdiServiceHost
Collected: ADMINISTRATORS,NT SERVICE\WdiServiceHost
Result: PASS

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (120659) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (120572) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data' (120798)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (120794)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Remotely accessible registry paths' (120600)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Collected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Result: PASS

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (120676)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (120737)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (120705)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (120587)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (120579)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (120624)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'EMET 5.5' or higher is installed (120755)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable screen saver' is set to 'Enabled' (120816)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Control Panel\Personalization\Enable screen saver
Result: PASS

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (120595)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (120519)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 14
Collected: 0
Result: FAIL

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (120815)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (120800)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (120683)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: C:\Program Files\LAPS\CSE\AdmPwd.dll
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (120566)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' (120771)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120613)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (120573)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Profile single process' is set to 'Administrators' (120552)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120654)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' (120799)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (120560)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 3
Collected: 0
Result: FAIL

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (120766)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 196608
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (120692)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely... (120690)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (120804)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (120525)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (120715)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (120602)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (120538)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (120697) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: <= 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on locally' to include 'Guests' (120540) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (120662) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (120632) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (120575) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (120561) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (120645) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (120594) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (120555) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (120714) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (120531) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (120574) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (120738) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (120604)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (120788)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (120517)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age
Result: FAIL

Compliance: Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled' (120823)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

User Configuration\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments
Result: PASS

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (120626)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (120627)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120764)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (120588)
N/A / tcp
unknown
Trivial
internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (120541)
N/A / tcp
unknown
Trivial
internal | **compliance** | **CIS auth**

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (120593)
N/A / tcp
unknown
Trivial
internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled' (120824)
N/A / tcp
unknown
Trivial
internal | **compliance** | **CIS auth**

User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile.
Result: PASS

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (120669)
N/A / tcp
unknown
Trivial
internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (120584)
N/A / tcp
unknown
Trivial
internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration
Result: PASS

Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (120712) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (120661) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_NONE Result: FAIL		
Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (120789) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (120674) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS Collected: AUDIT_SUCCESS Result: PASS		
Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (120565) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (120630) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120765) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (120606) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (120596) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (120591) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Audit Process Creation' is set to 'Success' (120664) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (120558) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (120622) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (120619) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: 0 Result: PASS		
Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (120681) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Configure 'Accounts: Rename guest account' (120564) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: not Guest Collected: Guest Result: FAIL		
Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (120522) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: >= 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (120782) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Default Protections for Recommended Software' is set to 'Enabled' (120759) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software Result: FAIL		
Compliance: Ensure 'Shut down the system' is set to 'Administrators' (120556) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (120656)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (120599)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (120612)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 1
Collected: 1
Result: PASS

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (120577)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Modify an object label' is set to 'No One' (120549)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (120670)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (120813)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' (120611)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (120605)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120768)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (120801)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallpublicfw.log' (120653)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: %systemroot%\system32\logfiles\firewall\publicfw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120810)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Logoff' is set to 'Success' (120668) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (120609) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' (120762) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (120615) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (120636) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (120562) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (120580) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit
Result: FAIL

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (120684)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (120743)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (120532)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (120752)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 255
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Protections for Internet Explorer' is set to 'Enabled' (120757)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: *\Internet Explorer\iexplore.exe
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Default Protections for Popular Software' is set to 'Enabled' (120758)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Computer Configuration\Administrative Templates\Windows Components\EMET\Default Protections for Popular Software
Result: FAIL

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (120763)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (120529)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (120741)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (120621)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 3
Result: FAIL

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (120534)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (120652)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (120544) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: Administrators Collected: ADMINISTRATORS Result: PASS		
Compliance: Configure 'Accounts: Rename administrator account' (120563) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: not Administrator Collected: Administrator Result: FAIL		
Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (120586) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 or 2 or 3 Collected: 0 Result: FAIL		
Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (120581) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: Any text Collected: Empty string Result: FAIL		
Compliance: Ensure 'Prevent the usage of SkyDrive for file storage' is set to 'Enabled' (120792) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (120803) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: 1 Result: PASS		
Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (120649) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (120808)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Account Lockout' is set to 'Success' (120667)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (120710)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (120770)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (120576)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age
Result: FAIL

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (120811)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (120614) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 537395200 Collected: 536870912 Result: FAIL		
Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (120734) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (120673) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_SUCCESS Result: FAIL		
Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (120640) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (120608) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 2147483644 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (120675) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: AUDIT_SUCCESS_FAILURE Collected: AUDIT_NONE Result: FAIL		

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (120718)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: PASS

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (120542)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (120520)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (120590)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (120807)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (120526)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (120568)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (120648)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (120516)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 24
Collected: 0
Result: FAIL

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (120694)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (120646)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (120795)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (120550)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (120603) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
	Expected: No Defined Values Collected: Not Defined Result: FAIL	
Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (120651) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
	Expected: 0 Collected: Not Defined Result: FAIL	
Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (120700) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
	Expected: <= 90 Collected: Not Defined Result: FAIL	
Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (120696) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
	Expected: 1 Collected: Not Defined Result: FAIL	
Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (120650) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
	Expected: 0 Collected: Not Defined Result: FAIL	
Compliance: Ensure 'Lock pages in memory' is set to 'No One' (120546) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial
	Expected: No One Collected: No One Result: PASS	
Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (120685) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (120688)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: <= 30
Collected: Not Defined
Result: FAIL

TLS Connection: TLS Version 1.1 Enabled (145426)
internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)
internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

SMB Native LanMan Version (100092)
internal | **recon** | **unauth**

139 / tcp
netbios

Trivial

LAN Manager: 6.3.9600.15
Domain: WIN-30QQRC10MGG
OS: Windows 2012 R2 Build 9600

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (120749)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (120784)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (120742)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120634) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (120644) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (120686) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (120543) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE
Result: PASS

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (120750) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (120530) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'System ASLR' is set to 'Enabled: Application Opt-In' (120760) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (120689) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (120677) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (120716) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security State Change' is set to 'Success' (120678) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Configure 'Manage auditing and security log' (120548) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (120680) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disa... (120691) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 2 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (120618) internal | compliance | CIS auth	N/A / tcp unknown	Trivial
Expected: 1 Collected: 0 Result: FAIL		

ATS-WIN-16 C

IP: 192.168.69.133
Asset name: ATS-WIN-16
Operating system: Windows Server 2016
Asset type: Server

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
smb	445 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Threat Scan: McAfee VirusScan Enterprise Disabled (127060) **internal | explicit | Threat Scan auth**	N/A / tcp unknown	Medium
The McAfee McShield service is not currently running.		
Threat Scan: Windows Defender Definitions Outdated (126741) **internal | explicit | Threat Scan auth**	N/A / tcp unknown	Medium
Definitions last updated: 05/19/2016 21:28:52 Detected definition version: 1.221.14.0		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.2 RC4-SHA - TLSv1.2		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp netbios	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1.2: DES-CBC3-SHA TLSv1.1: DES-CBC3-SHA TLSv1: DES-CBC3-SHA		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.2 RC4-SHA - TLSv1.2		

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
	[Large data section omitted]	
Compliance: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') (123114) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
	Expected: 255 Collected: 255 Result: PASS	
Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled' (123006) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
	Expected: 0 Collected: 0 Result: PASS	
Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled' (122959) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
	Expected: 0 Collected: 0 Result: PASS	
Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE' (123128) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
	Expected: 0 Collected: Not Defined Result: FAIL	
Compliance: Ensure 'Debug programs' is set to 'Administrators' (122914) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
	Expected: Administrators Collected: ADMINISTRATORS Result: PASS	
Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely ... (123085) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log' (123034) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled' (123108) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' (123028) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' (123049) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (123004) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Configure 'Enable computer and user accounts to be trusted for delegation' (122921) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Lock pages in memory' is set to 'No One' (122929) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account' (122920) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes' (123026) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' (123160) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled' (123245) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow LPT port redirection' is set to 'Enabled' (123214) internal | compliance | CIS auth	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Search Companion content file updates' is set to 'Enabled' (123139)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled' (123125)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop' (123011)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 2
Collected: 5
Result: FAIL

Compliance: Ensure 'Turn off multicast name resolution' is set to 'Enabled' (MS Only) (123097)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Input Personalization' is set to 'Disabled' (123077)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled' (123138)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' (123180)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled' (123121) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' (123211) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled' (122987) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: 0 Result: PASS		
Compliance: Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) (123167) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (122890) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: 0 Result: PASS		
Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE' (122924) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: LOCAL SERVICE,NETWORK SERVICE Collected: LOCAL SERVICE,NETWORK SERVICE Result: PASS		

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)' (123022)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled' (122974)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled' (122889)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) (122972)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled' (123229)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' (123141)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled' (123153)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled' (123223) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' (123043) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require pin for pairing' is set to 'Enabled' (123178) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Network access: Named Pipes that can be accessed anonymously' (122988) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: .+
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' (123124) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled' (123136) **internal** | **compliance** | **CIS auth**	N/A / tcp unknown	Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' (123054) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical' (123126) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' (123157) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)' (123029) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow COM port redirection' is set to 'Enabled' (123212) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)' (122891) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled' (122976) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (123246)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled' (123135)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled' (123089)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' (123070)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Audit Security State Change' is set to 'Success' (123072)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators' (122923)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled' (123000)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' (122907)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled' (123013)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Shut down the system' is set to 'Administrators' (122940)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No' (123042)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled' (122958)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only) (123161)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' (123031)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled' (123232)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' (123035)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' (123142)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Let Windows apps *' is set to 'Enabled: Force Deny' (123169)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' (123052)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM&NTLM' (123002)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 5
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Password Manager' is set to 'Disabled' (123201)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: no
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater' (123045)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' (122970)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: <= 14
Collected: 5
Result: PASS

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' (122956)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Untrusted Font Blocking' is set to 'Enabled: Block untrusted fonts and log events' (123154)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1000000000000
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types' (122999) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 2147483644
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled' (123152) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes' (123046) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled' (123179) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' (123074) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled' (123090) N/A / tcp unknown **Trivial**

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled' (123215)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on locally' to include 'Guests' (122919)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Configure Watson events' is set to 'Disabled' (123236)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE' (122938)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE
Result: PASS

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled' (123076)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) (123082)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' (123062)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (123190)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE' (123127)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' (122885)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: <= 60
Collected: 42
Result: PASS

Compliance: Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled' (123143)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled' (123014)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Configure 'Allow log on locally' (122901)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS,USERS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' (122908) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: Administrators Collected: ADMINISTRATORS Result: PASS		
Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves' (122995) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: 0 Result: PASS		
Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' (123259) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 0 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled' (123133) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: 1 Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log' (123024) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log Collected: Not Defined Result: FAIL		
Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log' (123044) **internal | compliance | CIS auth**	N/A / tcp unknown	Trivial
Expected: %systemroot%\system32\logfiles\firewall\publicfw.log Collected: Not Defined Result: FAIL		

Compliance: Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' (123164)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Accounts: Rename administrator account' (122947)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: not Administrator
Collected: Administrator
Result: FAIL

Compliance: Configure 'Manage auditing and security log' (122931)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' (122892)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 10
Collected: 0
Result: PASS

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' (122888)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 14
Collected: 0
Result: FAIL

Compliance: Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On' (123238)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled' (123193)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Back up files and directories' is set to 'Administrators' (122905) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' (123260) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable Windows NTP Client' is set to 'Enabled' (123166) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled' (123195) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled' (122952) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123185) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' (122935)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only) (122985)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled' (123110)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled' (123016)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (123094)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled' (123213)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled' (123150) N/A / tcp Trivial

internal | compliance | CIS auth

unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)' (123032) N/A / tcp Trivial

internal | compliance | CIS auth

unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled' (122997) N/A / tcp Trivial

internal | compliance | CIS auth

unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' (122994) N/A / tcp Trivial

internal | compliance | CIS auth

unknown

Expected: ^$
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (123186) N/A / tcp Trivial

internal | compliance | CIS auth

unknown

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' (123172) N/A / tcp Trivial

internal | compliance | CIS auth

unknown

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' (122942) N/A / tcp Trivial

internal | compliance | CIS auth

unknown

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE' (122906)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,LOCAL SERVICE
Collected: LOCAL SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled' (123196)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled' (123155)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled' (123242)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds' (123092)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: <= 5
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Access this computer from the network' (122896)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators,Authenticated Users
Collected: EVERYONE,ADMINISTRATORS,USERS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only) (122993)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: O:BAG:BAD:(A;;RC;;;BA)
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' (122960)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: > 0
Collected: 30
Result: PASS

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' (122898)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled' (123163)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' (123018)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123191)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Toggle user control over Insider builds' is set to 'Disabled' (123184) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123187) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled' (123132) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled' (123007) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' (123243) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' (123168) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Restore files and directories' is set to 'Administrators' (122939) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS,BACKUP OPERATORS
Result: FAIL

Compliance: Ensure 'Allow Use of Camera' is set to 'Disabled' (123176) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled' (123134) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Continue experiences on this device' is set to 'Disabled' (123129) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled' (123140) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow search and Cortana to use location' is set to 'Disabled' (123228) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' (123158) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled' (122981)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled' (123120)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled' (123100)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' (123244)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE' (122900)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' (123071)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS_FAILURE
Result: PASS

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes' (123037)
N/A / tcp
unknown
Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Process Creation' is set to 'Success' (123056) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party cookies' or higher (123200) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: <= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' (122934) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Audit Logoff' is set to 'Success' (123061) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled' (123087) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Audit Account Lockout' is set to 'Success and Failure' (123059) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater' (123188)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: >= 196608
Collected: Not Defined
Result: FAIL

Compliance: Set 'NetBIOS node type' to 'P-node' (Ensure NetBT Parameter 'NodeType' is set to '0x2 (2)') (MS Only) (123096)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 2
Collected: 2
Result: PASS

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled' (123149)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' (123221)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 60000
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less' (123095)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: <= 90
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled' (123222)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled' (123147)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' (122968)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: [a-zA-Z]
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only) (122982)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: >= 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Group Membership' is set to 'Success' (123060)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled' (123240)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' (123224)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Authorization Policy Change' is set to 'Success' (123068)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' (123192) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: >= 32768
Collected: Not Defined
Result: FAIL

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only) (123078) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: C:\Program Files\LAPS\CSE\AdmPwd.dll
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' (123039) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow InPrivate Browsing' is set to 'Disabled' (123199) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption' (123005) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 537395200
Collected: 536870912
Result: FAIL

Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' (123075) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' (122996) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' (122928)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only) (123081)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only) (122969)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: ^[43210]$
Collected: 10
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' (123030)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the Store application' is set to 'Enabled' (123233)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Extensions' is set to 'Disabled' (123198)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off access to the Store' is set to 'Enabled' (123131)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled' (122980)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators' (122927)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' (123241)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disable pre-release features or settings' is set to 'Disabled' (123182)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent using Localhost IP address for WebRTC' is set to 'Enabled' (123208)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Use enhanced anti-spoofing when available' is set to 'Enabled' (123175)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only) (123079) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3' (123093) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (123247) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled' (123227) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' (122950) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only) (123162) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only) (123122)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled' (122945)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: FAIL

Compliance: Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' (123237)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Modify an object label' is set to 'No One' (122933)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: No One
Collected: No One
Result: PASS

Compliance: Configure 'Allow log on through Remote Desktop Services' (122903)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators,Remote Desktop Users
Collected: ADMINISTRATORS,REMOTE DESKTOP USERS
Result: PASS

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled' (123159)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled' (122975)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' (122884)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: >= 24
Collected: 0
Result: FAIL

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled' (123017)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure' (123048)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' (123248)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' (122963)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)' (123033)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled' (123177)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off the advertising ID' is set to 'Enabled' (123165)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]' (123181)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' (123170)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' (123257)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' (123036)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands' (123173)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure' (123069)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled' (123084)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled' (122992)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Do not show feedback notifications' is set to 'Enabled' (123183)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled' (123091)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' (123021)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled' (123261)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Network access: Remotely accessible registry paths and sub-paths' (122991)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

[Large data section omitted]

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled' (122946)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' (123008)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled' (123209)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) (123123)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' (123231)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 4
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure' (123073) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' (123027) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Block launching Windows Store apps with Windows Runtime API access from hosted content.' is set to 'Enabled' (123171) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable insecure guest logons' is set to 'Disabled' (123099) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent bypassing SmartScreen prompts for sites' is set to 'Enabled' (123207) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' (123210) N/A / tcp unknown Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)' (122887) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes' (123041) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' (122957) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' (123156) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled' (123086) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 2
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Deny access to this computer from the network' (122915) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' (123015) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' (123063)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled' (122986)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Configure 'Network access: Remotely accessible registry paths' (122990)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: ^((System\\CurrentControlSet\\Control\\ProductOptions)|(System\\CurrentControlSet\\Control\\Server Applications)|(Software\\Microsoft\\Windows NT\\CurrentVersion))$
Collected: System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Server Applications
Software\Microsoft\Windows NT\CurrentVersion
Result: PASS

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled' (123010)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Enable Font Providers' is set to 'Disabled' (123098)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' (123019)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled' (122949)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit PNP Activity' is set to 'Success' (123055)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level' (123218)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)' (123040)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' (123066)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' (123038)

N/A / tcp
unknown

Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled' (123194) N/A / tcp Trivial
internal | compliance | CIS auth
unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic' (123145) N/A / tcp Trivial
internal | compliance | CIS auth
unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost' (122937) N/A / tcp Trivial
internal | compliance | CIS auth
unknown

Expected: Administrators,NT SERVICE\\WdiServiceHost
Collected: ADMINISTRATORS,NT SERVICE\WdiServiceHost
Result: PASS

Compliance: Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled' (123115) N/A / tcp Trivial
internal | compliance | CIS auth
unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Remote Shell Access' is set to 'Disabled' (123253) N/A / tcp Trivial
internal | compliance | CIS auth
unknown

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)' (123088) N/A / tcp Trivial
internal | compliance | CIS auth
unknown

Expected: 300000
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' (122911) N/A / tcp Trivial
internal | compliance | CIS auth
unknown

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) (123083)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: <= 30
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' (122979)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled' (122983)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0' (122977)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 15
Collected: 15
Result: PASS

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' (122943)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 1
Result: FAIL

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure' (123053)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Turn off printing over HTTP' is set to 'Enabled' (123137)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Cortana' is set to 'Disabled' (123225)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Create symbolic links' (122912)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' (122965)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: not 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Deny log on as a service' to include 'Guests' (122918)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes' (123047)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' (123067)
internal | compliance | CIS auth

N/A / tcp
unknown

Trivial

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares' (123112) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: [Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1.*[Rr]equire([Mm]utual[Aa]uthentication|[Ii]ntegrity)=1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Accounts: Rename guest account' (122948) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: not Guest
Collected: Guest
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' (123023) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' (123189) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled' (123216) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher (123003) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 1
Collected: 1
Result: PASS

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' (122894) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 15
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' (122910)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled' (123111)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled' (122964)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less' (123219)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: <= 900000
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Profile single process' is set to 'Administrators' (122936)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators
Collected: ADMINISTRATORS
Result: PASS

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' (122917)

internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Guests
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' (123148)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Disable all apps from Windows Store' is set to 'Enabled' (123230)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow remote server management through WinRM' is set to 'Disabled' (123250)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only) (122984)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests' (123012)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: 3
Result: FAIL

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' (123050)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_SUCCESS
Result: FAIL

Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' (122998) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled' (123104) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' (123251) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Special Logon' is set to 'Success' (123064) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS
Collected: AUDIT_SUCCESS
Result: PASS

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' (122951) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Select when Feature Updates are received' is set to 'Enabled: Current Branch for Business, 180 days' (123254) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent access to the about:flags page in Microsoft Edge' is set to 'Enabled' (123205) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Cortana above lock screen' is set to 'Disabled' (123226)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled' (123130)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: PASS

Compliance: Ensure 'Turn off Windows Error Reporting' is set to 'Enabled' (123144)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled' (123217)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) (123080)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prevent bypassing SmartScreen prompts for files' is set to 'Enabled' (123206)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' (123249)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts' (122944)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 3
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Join Microsoft MAPS' is set to 'Disabled' (123234)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: 0
Result: PASS

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled' (123252)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Impersonate a client after authentication' (122925)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: Administrators,LOCAL SERVICE,NETWORK SERVICE,SERVICE
Collected: LOCAL SERVICE,NETWORK SERVICE,ADMINISTRATORS,SERVICE
Result: PASS

Compliance: Ensure 'Turn off location' is set to 'Enabled' (123197)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure search suggestions in Address bar' is set to 'Disabled' (123203)
internal | **compliance** | **CIS auth**

N/A / tcp
unknown

Trivial

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure SmartScreen Filter' is set to 'Enabled' (123204)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled' (123109)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Create a token object' is set to 'No One' (122909)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' (123001)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 1
Result: PASS

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)' (123020)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' (123009)

N/A / tcp
unknown

Trivial

internal | **compliance** | **CIS auth**

Expected: 1
Collected: 0
Result: FAIL

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' (123174) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 255
Collected: Not Defined
Result: FAIL

Compliance: Configure 'Interactive logon: Message text for users attempting to log on' (122967) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: [a-zA-Z]
Collected: Empty string
Result: FAIL

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One' (122895) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: No One
Collected: No One
Result: PASS

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher (122973) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: ^(1|2|3)$
Collected: 0
Result: FAIL

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater' (123025) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: >= 16384
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled' (123151) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: 0
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Configure Pop-up Blocker' is set to 'Enabled' (123202) N/A / tcp unknown Trivial

internal | compliance | CIS auth

Expected: yes
Collected: Not Defined
Result: FAIL

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure' (123065) — N/A / tcp — unknown — Trivial

internal | compliance | CIS auth

Expected: AUDIT_SUCCESS_FAILURE
Collected: AUDIT_NONE
Result: FAIL

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' (122962) — N/A / tcp — unknown — Trivial

internal | compliance | CIS auth

Expected: 1
Collected: 1
Result: PASS

TLS Connection: TLS Version 1.0 Enabled (125641) — 3389 / tcp — msrdp — Trivial

internal | explicit | unauth

Server supports TLS version 1.0

SMB Native LanMan Version (100092) — 139 / tcp — netbios — Trivial

internal | recon | unauth

LAN Manager: 10.0.14393.15
Domain: ATS
OS: Windows 2016 Build 14393

tplinkmodem.net — B

IP: 10.1.1.1
Asset name: tplinkmodem.net
Operating system: unknown
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
http (ssl)	443 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) internal | explicit | unauth	443 / tcp http (ssl)	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-SHA - TLSv1.2 RC4-MD5 - TLSv1.2		
SSL Connection: Sweet32 Vulnerability (121110) internal | explicit | unauth	443 / tcp http (ssl)	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1.2: DES-CBC3-SHA IDEA-CBC-SHA		
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) internal | explicit | unauth	443 / tcp http (ssl)	Trivial
SSL connection supports the following SSL/TLS RC4 ciphers: RC4-SHA - TLSv1.2 RC4-MD5 - TLSv1.2		
Content Security Policy Missing (148043) internal | explicit | unauth	443 / tcp http (ssl)	Trivial
Missing Content Security Policy.		
SSL Certificate: Chain Contains Weak RSA Keys (104022) internal | explicit | unauth	443 / tcp http (ssl)	Trivial
Inadequate Certificate Key Size: 1024		
Content Security Policy Missing (148043) internal | explicit | unauth	80 / tcp http	Trivial
Missing Content Security Policy.		

192.168.0.1	B

IP: 192.168.0.1
Asset name: 192.168.0.1
Operating system: unknown
Asset type: Server

Protocol	Service
http	80 / tcp
http (ssl)	443 / tcp
http	1900 / tcp
ssh	20001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Certificate: Chain Contains Weak RSA Keys (104022) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Trivial
Inadequate Certificate Key Size: 1024		
SSL Connection: TLS Compression Enabled (112280) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Trivial
TLS Supports DEFLATE compression		

_gateway B

IP: 192.168.0.1
Asset name: _gateway
Operating system: unknown
Asset type: Firewall

Protocol	Service
dns	53 / udp
unknown	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

TP-SHARE	B

IP: 192.168.0.2
Asset name: TP-SHARE
Operating system: unknown
Asset type: Device

Protocol	Service
http	80 / tcp
netbios-ns	137 / udp
http (ssl)	443 / tcp
ssh	20001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: TLS Compression Enabled (112280) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
TLS Supports DEFLATE compression		
SSL Certificate: Chain Contains Weak RSA Keys (104022) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Inadequate Certificate Key Size: 1024		

192.168.0.12	B

IP: 192.168.0.12
Asset name: 192.168.0.12
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.0.100	B

IP: 192.168.0.100
Asset name: 192.168.0.100
Operating system: Linux Variant
Asset type: Server

Protocol	Service
http	80 / tcp
http	49152 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.0.108 | B

IP: 192.168.0.108
Asset name: 192.168.0.108
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

DB-WINSERV16 | B

IP: 192.168.0.110
Asset name: DB-WINSERV16
Operating system: Windows Server 2016
Asset type: Server

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
tds	1433 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	1433 / tcp tds	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-SHA - TLSv1.2 RC4-MD5 - TLSv1.2		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.2 RC4-SHA - TLSv1.2		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp netbios	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1.2: DES-CBC3-SHA TLSv1.1: DES-CBC3-SHA TLSv1: DES-CBC3-SHA		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	1433 / tcp tds	Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

1433 / tcp
tds

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-SHA - TLSv1.2
RC4-MD5 - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

1433 / tcp
tds

Trivial

[Large data section omitted]

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

1433 / tcp
tds

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) internal | explicit | unauth	3389 / tcp msrdp	Trivial
	Server supports TLS version 1.1	
TDS SQL Database Service (101436) internal | recon | unauth	1433 / tcp tds	Trivial
	TDS SQL database service detected	
TLS Connection: TLS Version 1.1 Enabled (145426) internal | explicit | unauth	1433 / tcp tds	Trivial
	Server supports TLS version 1.1	
SMB Native LanMan Version (100092) internal | recon | unauth	139 / tcp netbios	Trivial
	LAN Manager: 10.0.14393.15 Domain: ISMAILDOMAIN OS: Windows 2016 Build 14393	

TE-WINSERV16 B

IP: 192.168.0.111
Asset name: TE-WINSERV16
Operating system: Windows Server 2016
Asset type: Server

Protocol	Service
http	80 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
http (ssl)	443 / tcp
tds	1433 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	8080 / tcp
http	47001 / tcp

unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.2 RC4-SHA - TLSv1.2		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	1433 / tcp tds	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-SHA - TLSv1.2 RC4-MD5 - TLSv1.2		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp netbios	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

SSL Connection: Sweet32 Vulnerability (121110)

internal | **explicit** | **unauth**

1433 / tcp
tds

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | **explicit** | **unauth**

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

1433 / tcp
tds

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | **explicit** | **unauth**

1433 / tcp
tds

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-SHA - TLSv1.2
RC4-MD5 - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
DHE-RSA-AES256-SHA - TLSv1
AES256-SHA - TLSv1
AES128-SHA - TLSv1
DHE-RSA-AES128-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

Content Security Policy Missing (148043)

internal | explicit | unauth

80 / tcp
http

Trivial

Missing Content Security Policy.

Default IIS Webpage Detected (117366)

internal | recon | unauth

80 / tcp
http

Trivial

Default IIS Webpage Detected

SMB Native LanMan Version (100092)

internal | recon | unauth

139 / tcp
netbios

Trivial

LAN Manager: 10.0.14393.15
Domain: ISMAILDOMAIN
OS: Windows 2016 Build 14393

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

1433 / tcp
tds

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	1433 / tcp tds	Trivial
Server supports TLS version 1.0		
TDS SQL Database Service (101436) **internal | recon | unauth**	1433 / tcp tds	Trivial
TDS SQL database service detected		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Server supports TLS version 1.1		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
Server supports TLS version 1.0		

192.168.0.115 B

IP: 192.168.0.115
Asset name: 192.168.0.115
Operating system: unknown
Asset type: Server

Protocol	Service
ssh	22 / tcp
rpcbind	111 / tcp
rpcbind	111 / udp
msrdp	3389 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity

RPC Portmap Service (100505) **internal | explicit | unauth**	111 / udp rpcbind	Trivial
	Not Applicable	
RPC Portmap Service (100505) **internal | explicit | unauth**	111 / tcp rpcbind	Trivial
	Not Applicable	
Remote Desktop Protocol Allows Man in the Middle (117858) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
	rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)	
TLS Connection: TLS Version 1.2 Not Enabled (146258) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
	Server does not support TLS version 1.2	

192.168.0.120 B

IP: 192.168.0.120
Asset name: 192.168.0.120
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.0.121 B

IP: 192.168.0.121
Asset name: 192.168.0.121
Operating system: unknown

Asset type: Device

Protocol	Service
ssh	22 / tcp
msrdp	3389 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Remote Desktop Protocol Allows Man in the Middle (117858) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)		
TLS Connection: TLS Version 1.2 Not Enabled (146258) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
Server does not support TLS version 1.2		

192.168.0.129 B

IP: 192.168.0.129
Asset name: 192.168.0.129
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

WIN-SERV16-D2	B

IP: 192.168.0.150
Asset name: WIN-SERV16-D2
Operating system: Windows Server 2016
Asset type: Server

Protocol	Service
echo	7 / tcp
unknown	7 / udp
discard	9 / tcp
daytime	13 / tcp
quote	17 / tcp
chargen	19 / tcp
ssh	22 / tcp
http	80 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
tds	1433 / tcp
msrdp	3389 / tcp
postgresql (ssl)	5432 / tcp
winrm	5985 / tcp
http (ssl)	8091 / tcp
http	10443 / tcp
http	47001 / tcp

unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) internal | explicit | unauth	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-SHA - TLSv1 RC4-MD5 - TLSv1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.2 RC4-MD5 - TLSv1.2		
Quote Of The Day Service (100935) internal | recon | unauth	17 / tcp quote	Low
"Here's the rule for bargains: "Do other men, for they would do you." That's the true business precept." Charles Dickens (1812-70)		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) internal | explicit | unauth	8091 / tcp http (ssl)	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-SHA - TLSv1.2 RC4-MD5 - TLSv1.2		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) internal | explicit | unauth	1433 / tcp tds	Low

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SMB Security Signatures Not Required (104188)
internal | explicit | unauth

139 / tcp
netbios

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

Discard Service Detected (100370)
internal | recon | unauth

9 / tcp
discard

Trivial

Not Applicable

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

Echo Service (101032)
internal | explicit | unauth

7 / tcp
echo

Trivial

echo server detected

Echo Service (101032)
internal | explicit | unauth

7 / udp
unknown

Trivial

echo server detected

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth

8091 / tcp
http (ssl)

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

Chargen Service (101021)

internal | recon | unauth

19 / tcp
chargen

Trivial

[Large data section omitted]

Daytime Service Detected (101026)

internal | recon | unauth

13 / tcp
daytime

Trivial

7:14:06 PM 10/4/2022

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

1433 / tcp
tds

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - TLSv1
RC4-MD5 - TLSv1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.2
RC4-MD5 - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

1433 / tcp
tds

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

1433 / tcp
tds

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

8091 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

8091 / tcp
http (ssl)

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-SHA - TLSv1.2
RC4-MD5 - TLSv1.2

Content Security Policy Missing (148043)

internal | explicit | unauth

80 / tcp
http

Trivial

Missing Content Security Policy.

NTLM Authentication Host Information Disclosure (117943)

internal | recon | unauth

80 / tcp
http

Trivial

NetBIOS Domain: ISMAILDOMAIN
NetBIOS Hostname: WIN-SERV16-D2
DNS Domain Name: ismaildomain.lab
DNS Hostname: WIN-Serv16-D2.ismaildomain.lab

Default IIS Webpage Detected (117366)

internal | recon | unauth

80 / tcp
http

Trivial

Default IIS Webpage Detected

SMB Native LanMan Version (100092)

internal | recon | unauth

139 / tcp
netbios

Trivial

LAN Manager: 10.0.14393.15
Domain: ISMAILDOMAIN
OS: Windows 2016 Build 14393

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.1		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	1433 / tcp tds	Trivial
Server supports TLS version 1.0		
TDS SQL Database Service (101436) **internal | recon | unauth**	1433 / tcp tds	Trivial
TDS SQL database service detected		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	8091 / tcp http (ssl)	Trivial
Server supports TLS version 1.1		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	8091 / tcp http (ssl)	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	1433 / tcp tds	Trivial
Server supports TLS version 1.1		

TDC-NODE B

IP: 192.168.0.151
Asset name: TDC-NODE
Operating system: Windows Server 2016
Asset type: Server

Protocol	**Service**
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
http (ssl)	443 / tcp

msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-SHA - TLSv1 RC4-MD5 - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.2 RC4-SHA - TLSv1.2		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	443 / tcp http (ssl)	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-MD5 - TLSv1 RC4-SHA - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-SHA - TLSv1.2 RC4-MD5 - TLSv1.2		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp netbios	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial

Weak Signature Algorithm: SHA-1

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - TLSv1
RC4-MD5 - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-SHA - TLSv1.2
RC4-MD5 - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)
internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

[Large data section omitted]

Content Security Policy Missing (148043)
internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Missing Content Security Policy.

TLS Connection: TLS Version 1.1 Enabled (145426)
internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)
internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)
internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)
internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.0

SMB Native LanMan Version (100092)
internal | recon | unauth

139 / tcp
netbios

Trivial

LAN Manager: 10.0.14393.15
Domain: ISMAILDOMAIN
OS: Windows 2016 Build 14393

192.168.0.155 B

IP: 192.168.0.155
Asset name: 192.168.0.155
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

TE-WD-SECONDARY	B

IP: 192.168.0.157
Asset name: TE-WD-SECONDARY
Operating system: Windows Server 2016
Asset type: Server

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
tds	1433 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	3389 / tcp msrdp	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-SHA - TLSv1 RC4-MD5 - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-SHA - TLSv1.2 RC4-MD5 - TLSv1.2		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	1433 / tcp tds	Low
Vulnerable to Bar Mitzvah attack. SSL connection supports the following SSL/TLS RC4 ciphers: RC4-SHA - TLSv1 RC4-MD5 - TLSv1 RC4-MD5 - TLSv1.1 RC4-SHA - TLSv1.1 RC4-MD5 - TLSv1.2 RC4-SHA - TLSv1.2		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp netbios	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	1433 / tcp tds	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1.2: DES-CBC3-SHA TLSv1.1: DES-CBC3-SHA TLSv1: DES-CBC3-SHA		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - TLSv1
RC4-MD5 - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-SHA - TLSv1.2
RC4-MD5 - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

1433 / tcp
tds

Trivial

internal | **explicit** | **unauth**

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

1433 / tcp
tds

Trivial

internal | **explicit** | **unauth**

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - TLSv1
RC4-MD5 - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

TLS Connection: TLS Version 1.1 Enabled (145426)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)

3389 / tcp
msrdp

Trivial

internal | **explicit** | **unauth**

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	1433 / tcp tds	Trivial
	Server supports TLS version 1.1	
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	1433 / tcp tds	Trivial
	Server supports TLS version 1.0	
TDS SQL Database Service (101436) **internal | recon | unauth**	1433 / tcp tds	Trivial
	TDS SQL database service detected	
SMB Native LanMan Version (100092) **internal | recon | unauth**	139 / tcp netbios	Trivial
	LAN Manager: 10.0.14393.15 Domain: ISMAILDOMAIN OS: Windows 2016 Build 14393	

TE.GALAXY.FFA — B

IP: 192.168.0.160
Asset name: TE.GALAXY.FFA
Operating system: unknown
Asset type: Server

Protocol	Service
ssh	22 / tcp
smtp	25 / tcp
http (ssl)	443 / tcp
msrdp	3389 / tcp
http	8080 / tcp
http (ssl)	8100 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
PHP End of Life (112906) **internal | explicit | unauth**	8100 / tcp http (ssl)	Low
Version 5.4.16 of PHP has reached end-of-life status.		
SMTP Server EXPN/VRFY (100876) **internal | explicit | unauth**	25 / tcp smtp	Low
VRFY root: 252 2.0.0 root		
Remote Desktop Protocol Allows Man in the Middle (117858) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
rdp5 server does not require ssl and is vulnerable to mitm attack (CVE-2005-1794)		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	8100 / tcp http (ssl)	Trivial
SSL connection supports the following SSLv3/TLSv1 CBC mode cipher: ECDHE-RSA-AES256-SHA - TLSv1 DHE-RSA-AES256-SHA - TLSv1 BEAST not mitigated: all supported ciphers are CBC mode ciphers		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial
SSL connection supports the following SSLv3/TLSv1 CBC mode cipher: AES128-SHA - TLSv1 DHE-RSA-AES256-SHA - TLSv1 AES256-SHA - TLSv1 DHE-RSA-AES128-SHA - TLSv1 BEAST not mitigated: all supported ciphers are CBC mode ciphers		
TLS Connection: TLS Version 1.2 Not Enabled (146258) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
Server does not support TLS version 1.2		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	8100 / tcp http (ssl)	Trivial
Server supports TLS version 1.1		

TLS Connection: TLS Version 1.0 Enabled (125641) **internal** | **explicit** | **unauth**	8100 / tcp http (ssl)	Trivial
Server supports TLS version 1.0		
SSL Certificate: Expired Certificate Date (103615) **internal** | **explicit** | **unauth**	8100 / tcp http (ssl)	Trivial
Date Appears Invalid: Sep 23 16:58:11 2019 GMT to Sep 22 16:58:11 2021 GMT		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Trivial
Server supports TLS version 1.1		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Trivial
Server supports TLS version 1.0		

WIN-FNLDRQ86328 — B

IP: 192.168.0.167
Asset name: WIN-FNLDRQ86328
Operating system: Windows Platform
Asset type: Server

Protocol	Service
netbios-ns	137 / udp
msrdp	3389 / tcp
winrm	5985 / tcp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Low

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - TLSv1
RC4-MD5 - TLSv1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.2
RC4-MD5 - TLSv1.2

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.2:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-SHA - TLSv1
RC4-MD5 - TLSv1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.2
RC4-MD5 - TLSv1.2

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

[Large data section omitted]

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

3389 / tcp
msrdp

Trivial

Server supports TLS version 1.1

HSATP-7WRCTG3 — B

IP: 192.168.0.173
Asset name: HSATP-7WRCTG3
Operating system: unknown
Asset type: Unknown

Protocol	Service
smtp	25 / tcp
netbios-ns	137 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Protocol Allows Authentication Over Clear Text (104798) **internal** | **explicit** | **unauth**	25 / tcp smtp	Low
smtp allows transmission of credentials in clear text		

192.168.0.175 **B**

IP: 192.168.0.175
Asset name: 192.168.0.175
Operating system: CentOS
Asset type: Server

Protocol	Service
ssh	22 / tcp
http (ssl)	443 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
HTTP Host Header Value Reflection (128596) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Low

/ : a href="https://vm.frontline.cloud/index.ice">here

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) internal | explicit | unauth	443 / tcp http (ssl)	Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
ECDHE-RSA-AES256-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
AES256-SHA - TLSv1
DHE-RSA-AES256-SHA - TLSv1
AES128-SHA - TLSv1
DHE-RSA-AES128-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

Content Security Policy Missing (148043) internal | explicit | unauth	443 / tcp http (ssl)	Trivial

Missing Content Security Policy.

Apache Server Header Information Disclosure (123916) internal | recon | unauth	443 / tcp http (ssl)	Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2zb-fips mod_wsgi/4.6.4 Python/2.7

TLS Connection: TLS Version 1.1 Enabled (145426) internal | explicit | unauth	443 / tcp http (ssl)	Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641) internal | explicit | unauth	443 / tcp http (ssl)	Trivial

Server supports TLS version 1.0

192.168.0.194	**B**

IP: 192.168.0.194
Asset name: 192.168.0.194
Operating system: unknown
Asset type: Unknown

Protocol	Service
http	7676 / tcp
http	8080 / tcp
unknown	N/A / tcp

unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.0.199 B

IP: 192.168.0.199
Asset name: 192.168.0.199
Operating system: unknown
Asset type: Device

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
HTTP XML Injection (104276) **internal | explicit | unauth**	80 / tcp http	Low
Possible XML injection(s) found: 192.168.0.199:80: Responses differ : /nirv>'>"><nirv></nirv> and /nirv>'>"></nirv><nirv>		
Apache ETags Inode Number Disclosure (121914) **internal | explicit | unauth**	80 / tcp http	Trivial

The instance of Apache running on this asset at TCP port 80 discloses inode numbers in ETag header fields:

ETag Header Value: 3db-110-5996706f
Inode Number: 987
File Size: 272 bytes
Last Modified (Epoch): 1503031407

192.168.0.210 B

IP: 192.168.0.210
Asset name: 192.168.0.210
Operating system: unknown
Asset type: Unknown

Protocol	Service
http	8008 / tcp
unknown (ssl)	8009 / tcp
http (ssl)	8443 / tcp
unknown (ssl)	10101 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	8009 / tcp unknown (ssl)	Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

TLSv1:
DES-CBC3-SHA

Vulnerability Title	Service(s)	Severity
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	8443 / tcp http (ssl)	Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

8009 / tcp
unknown (ssl)

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

8443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

8009 / tcp
unknown (ssl)

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

8009 / tcp
unknown (ssl)

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

8443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

10101 / tcp
unknown (ssl)

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

10101 / tcp
unknown (ssl)

Trivial

Server supports TLS version 1.0

192.168.0.238 B

IP: 192.168.0.238
Asset name: 192.168.0.238

Operating system: unknown
Asset type: Unknown

Protocol	Service
http	8008 / tcp
unknown (ssl)	8009 / tcp
http (ssl)	8443 / tcp
unknown (ssl)	10101 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal | explicit | unauth**	8443 / tcp http (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	8009 / tcp unknown (ssl)	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1: DES-CBC3-SHA TLSv1.2: DES-CBC3-SHA TLSv1.1: DES-CBC3-SHA		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	8009 / tcp unknown (ssl)	Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

8443 / tcp
http (ssl)

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | **explicit** | **unauth**

8443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | **explicit** | **unauth**

8443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | **explicit** | **unauth**

8009 / tcp
unknown (ssl)

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | **explicit** | **unauth**

8009 / tcp
unknown (ssl)

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | **explicit** | **unauth**

10101 / tcp
unknown (ssl)

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | **explicit** | **unauth**

10101 / tcp
unknown (ssl)

Trivial

Server supports TLS version 1.1

192.168.1.1 B

IP: 192.168.1.1
Asset name: 192.168.1.1

Operating system: unknown
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
http (ssl)	443 / tcp
http	8000 / tcp
http	8080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Certificate: Weak Signature Algorithm SHA-1 (121119) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Trivial
Weak Signature Algorithm: SHA-1		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Trivial
Server supports TLS version 1.1		

192.168.1.33 B

IP: 192.168.1.33
Asset name: 192.168.1.33
Operating system: unknown
Asset type: Device

Protocol	Service
http	80 / tcp
unknown (ssl)	443 / tcp

unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal** | **explicit** | **unauth**	443 / tcp unknown (ssl)	Trivial
SSL connection supports the following SSLv3/TLSv1 CBC mode cipher: AES128-SHA - TLSv1 AES256-SHA - TLSv1 BEAST not mitigated: all supported ciphers are CBC mode ciphers		
SSL Certificate: Expired Certificate Date (103615) **internal** | **explicit** | **unauth**	443 / tcp unknown (ssl)	Trivial
Date Appears Invalid: Jun 23 15:19:13 2017 GMT to Jun 24 15:19:13 2020 GMT		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal** | **explicit** | **unauth**	443 / tcp unknown (ssl)	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal** | **explicit** | **unauth**	443 / tcp unknown (ssl)	Trivial
Server supports TLS version 1.1		

DESKTOP-FV6DPRC — B

IP: 192.168.1.48
Asset name: DESKTOP-FV6DPRC
Operating system: Windows 10 Enterprise
Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp

smb	445 / tcp
msrdp	3389 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SMB Security Signatures Not Required (104188) **internal** | **explicit** | **unauth**	445 / tcp smb	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SMB Null Session Authentication (101373) **internal** | **recon** | **unauth**	445 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		
SSL Connection: Sweet32 Vulnerability (121110) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1: DES-CBC3-SHA TLSv1.1: DES-CBC3-SHA TLSv1.2: DES-CBC3-SHA		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
SSL connection supports the following SSLv3/TLSv1 CBC mode cipher: AES128-SHA - TLSv1 AES256-SHA - TLSv1 DES-CBC3-SHA - TLSv1 ECDHE-RSA-AES128-SHA - TLSv1 ECDHE-RSA-AES256-SHA - TLSv1 BEAST not mitigated: all supported ciphers are CBC mode ciphers		

SMB Native LanMan Version (100092) **internal | recon | unauth**	445 / tcp smb	Trivial
	LAN Manager: Windows 10 Enterprise 6.3 Domain: WORKGROUP OS: Windows 10 Enterprise 19042	
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
	Server supports TLS version 1.0	
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial
	Server supports TLS version 1.1	

192.168.67.48	**B**

IP: 192.168.67.48
Asset name: 192.168.67.48
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.57	**B**

IP: 192.168.67.57
Asset name: 192.168.67.57
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.59	**B**

IP: 192.168.67.59
Asset name: 192.168.67.59
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.62	**B**

IP: 192.168.67.62
Asset name: 192.168.67.62
Operating system: CentOS
Asset type: Server

Protocol	Service

ftp	21 / tcp
ssh	22 / tcp
http	80 / tcp
mysql	3306 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Web Server Directory Indexing Enabled (101049) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Directory Indexing Enabled: 192.168.67.62:80: /icons /icons/small		
Apache Username Disclosure (101469) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Apache username disclosure detected: /~root		
Slowloris Resource Depletion And Denial Of Service (117854) **internal** | **explicit** | **unauth**	80 / tcp http	Low
The webserver appears to be vulnerable to a resource exhaustion attack.		
Phpinfo.php System Information Disclosure (100403) **internal** | **explicit** | **unauth**	80 / tcp http	Low
[Large data section omitted]		
Product Has Reached End-of-Life Status (104220) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Version 2.2.15 of the Apache Web Server has reached end-of-life status.		
Apache Default Start Page (103388) **internal** | **recon** | **unauth**	80 / tcp http	Low

Unconfigured Apache server detected		
PHP End of Life (112906) **internal | explicit | unauth**	80 / tcp http	Low
Version 5.3.3 of PHP has reached end-of-life status.		
Anonymous FTP Enabled (101362) **internal | explicit | unauth**	21 / tcp ftp	Low
anonymous		
HTTP TRACE/TRACK Method Enabled (117856) **internal | explicit | unauth**	80 / tcp http	Trivial
Not Applicable		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		

192.168.67.63 B

IP: 192.168.67.63
Asset name: 192.168.67.63
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Ubuntu End of Life (117365) **internal | explicit | unauth**	N/A / tcp unknown	Low
Ubuntu 12.04 has reached end-of-life status.		

192.168.67.63 B

IP: 192.168.67.63
Asset name: 192.168.67.63
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Ubuntu End of Life (117365) **internal** | **explicit** | **unauth**	N/A / tcp unknown	Low

Ubuntu 12.04 has reached end-of-life status.

192.168.67.64 B

IP: 192.168.67.64
Asset name: 192.168.67.64
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp
mysql	3306 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Anonymous FTP Enabled (101362) **internal | explicit | unauth**	21 / tcp ftp	Low

anonymous

UBUNTU-14-SERVE	B

IP: 192.168.67.67
Asset name: UBUNTU-14-SERVE
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
http	80 / tcp
pop3	110 / tcp
netbios-ns	137 / udp
smb	139 / tcp
imap	143 / tcp
imap (ssl)	993 / tcp
pop3 (ssl)	995 / tcp
iax2	4569 / udp
http	8080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	995 / tcp pop3 (ssl)	Low
[Large data section omitted]		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	110 / tcp pop3	Low
[Large data section omitted]		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	993 / tcp imap (ssl)	Low
[Large data section omitted]		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	143 / tcp imap	Low
[Large data section omitted]		
Slowloris Resource Depletion And Denial Of Service (117854) **internal** | **explicit** | **unauth**	8080 / tcp http	Low
The webserver appears to be vulnerable to a resource exhaustion attack.		
SMB Security Signatures Not Required (104188) **internal** | **explicit** | **unauth**	139 / tcp smb	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SSL Connection: SSL Version 3 Enabled (128440) **internal** | **explicit** | **unauth**	143 / tcp imap	Low
Server supports SSL version 3		
SSL Connection: SSL Version 3 Enabled (128440) **internal** | **explicit** | **unauth**	993 / tcp imap (ssl)	Low
Server supports SSL version 3		

SMB User Enumeration (113348)
internal | explicit | unauth

139 / tcp
smb

Low

Users for domain 'UBUNTU-14-SERVER':
buff

ISC BIND End Of Life (123915)
internal | explicit | unauth

53 / tcp
dns

Low

ISC Bind version 9.9.5 has surpassed its EOL date.

SSL Connection: SSL Version 3 Enabled (128440)
internal | explicit | unauth

995 / tcp
pop3 (ssl)

Low

Server supports SSL version 3

SSL Connection: SSL Version 3 Enabled (128440)
internal | explicit | unauth

110 / tcp
pop3

Low

Server supports SSL version 3

ISC BIND End Of Life (123915)
internal | explicit | unauth

53 / udp
dns

Low

ISC Bind version 9.9.5 has surpassed its EOL date.

SMB Null Session Authentication (101373)
internal | recon | unauth

139 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth

995 / tcp
pop3 (ssl)

Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth

993 / tcp
imap (ssl)

Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth

110 / tcp
pop3

Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)
internal | explicit | unauth

143 / tcp
imap

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)
internal | **explicit** | **unauth**

995 / tcp
pop3 (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)
internal | **explicit** | **unauth**

143 / tcp
imap

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | **explicit** | **unauth**

143 / tcp
imap

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)
internal | **explicit** | **unauth**

993 / tcp
imap (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | **explicit** | **unauth**

993 / tcp
imap (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | **explicit** | **unauth**

995 / tcp
pop3 (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)
internal | **explicit** | **unauth**

110 / tcp
pop3

Trivial

[Large data section omitted]

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)
internal | **explicit** | **unauth**

110 / tcp
pop3

Trivial

[Large data section omitted]

Content Security Policy Missing (148043)
internal | **explicit** | **unauth**

80 / tcp
http

Trivial

Missing Content Security Policy.

Content Security Policy Missing (148043) 8080 / tcp Trivial
internal | explicit | unauth http

Missing Content Security Policy.

TLS Connection: TLS Version 1.0 Enabled (125641) 143 / tcp Trivial
internal | explicit | unauth imap

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) 143 / tcp Trivial
internal | explicit | unauth imap

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641) 993 / tcp Trivial
internal | explicit | unauth imap (ssl)

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) 993 / tcp Trivial
internal | explicit | unauth imap (ssl)

Server supports TLS version 1.1

SMB Native LanMan Version (100092) 139 / tcp Trivial
internal | recon | unauth smb

LAN Manager: Samba 4.3.9-Ubuntu
Domain: WORKGROUP
OS: Windows 6.1

Default Apache Tomcat Webpage Detected (117554) 8080 / tcp Trivial
internal | recon | unauth http

Default Apache Tomcat 6 webpage detected

TLS Connection: TLS Version 1.0 Enabled (125641) 995 / tcp Trivial
internal | explicit | unauth pop3 (ssl)

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) 995 / tcp Trivial
internal | explicit | unauth pop3 (ssl)

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641) **internal** | **explicit** | **unauth**	110 / tcp pop3	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal** | **explicit** | **unauth**	110 / tcp pop3	Trivial
Server supports TLS version 1.1		
Web Server Default Error Page Detected (128223) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial
[Large data section omitted]		

UBUNTU-16-SERVE — B

IP: 192.168.67.69
Asset name: UBUNTU-16-SERVE
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
http	80 / tcp
pop3	110 / tcp
netbios-ns	137 / udp
smb	139 / tcp
imap	143 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp smb	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SMB Null Session Authentication (101373) **internal | recon | unauth**	139 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		
SMB Native LanMan Version (100092) **internal | recon | unauth**	139 / tcp smb	Trivial
LAN Manager: Samba 4.3.11-Ubuntu Domain: WORKGROUP OS: Windows 6.1		

192.168.67.74 B

IP: 192.168.67.74
Asset name: 192.168.67.74
Operating system: CentOS
Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp
http	80 / tcp
mysql	3306 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Web Server Directory Indexing Enabled (101049) internal | explicit | unauth	80 / tcp http	Low
Directory Indexing Enabled: 192.168.67.74:80: /icons /icons/small		
Slowloris Resource Depletion And Denial Of Service (117854) internal | explicit | unauth	80 / tcp http	Low
The webserver appears to be vulnerable to a resource exhaustion attack.		
Product Has Reached End-of-Life Status (104220) internal | explicit | unauth	80 / tcp http	Low
Version 2.2.15 of the Apache Web Server has reached end-of-life status.		
Apache Default Start Page (103388) internal | recon | unauth	80 / tcp http	Low
Unconfigured Apache server detected		
PHP End of Life (112906) internal | explicit | unauth	80 / tcp http	Low
Version 5.3.3 of PHP has reached end-of-life status.		
Anonymous FTP Enabled (101362) internal | explicit | unauth	21 / tcp ftp	Low
anonymous		
HTTP TRACE/TRACK Method Enabled (117856) internal | explicit | unauth	80 / tcp http	Trivial
Not Applicable		
Web Server Default Error Page Detected (128223) internal | explicit | unauth	80 / tcp http	Trivial
[Large data section omitted]		

192.168.67.75 — B

IP: 192.168.67.75
Asset name: 192.168.67.75
Operating system: Linux Variant

Asset type: Server

Protocol	Service
ssh	22 / tcp
http (ssl)	81 / tcp
http	82 / tcp
http (ssl)	83 / tcp
smb	139 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
HTTP Host Header Value Reflection (128596) **internal** | **explicit** | **unauth**	81 / tcp http (ssl)	Low
/app/base/session/login/L2FwcC9iYXNlLw__ : action="https://vm.frontline.cloud/app/base/sessio /app/base/session/login/text/ : action="https://vm.frontline.cloud/app/base/sessio		
HTTP Host Header Value Reflection (128596) **internal** | **explicit** | **unauth**	82 / tcp http	Low
/app/base/session/login/L2FwcC9iYXNlLw__ : action="http://vm.frontline.cloud/app/base/sessio		
SMB User Enumeration (113348) **internal** | **explicit** | **unauth**	139 / tcp smb	Low
Users for domain 'CLEAROS': admin		
SSL Connection: SSL Version 3 Enabled (128440) **internal** | **explicit** | **unauth**	81 / tcp http (ssl)	Low
Server supports SSL version 3		

SSL Connection: Sweet32 Vulnerability (121110)

internal | **explicit** | **unauth**

81 / tcp
http (ssl)

Trivial

[Large data section omitted]

SMB Null Session Authentication (101373)

internal | **recon** | **unauth**

139 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

SSL Connection: Sweet32 Vulnerability (121110)

internal | **explicit** | **unauth**

83 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

81 / tcp
http (ssl)

Trivial

[Large data section omitted]

Web Server Default Error Page Detected (128223)

internal | **explicit** | **unauth**

83 / tcp
http (ssl)

Trivial

[Large data section omitted]

Apache Server Header Information Disclosure (123916)

internal | **recon** | **unauth**

83 / tcp
http (ssl)

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (ClearOS) OpenSSL/1.0.2k-fips

Apache Server Header Information Disclosure (123916)

internal | **recon** | **unauth**

82 / tcp
http

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (ClearOS) OpenSSL/1.0.2k-fips

Web Server Default Error Page Detected (128223)

internal | **explicit** | **unauth**

81 / tcp
http (ssl)

Trivial

[Large data section omitted]

Web Server Default Error Page Detected (128223)

internal | **explicit** | **unauth**

82 / tcp
http

Trivial

[Large data section omitted]

Apache Server Header Information Disclosure (123916)

internal | **recon** | **unauth**

81 / tcp
http (ssl)

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (ClearOS) OpenSSL/1.0.2k-fips

SMB Native LanMan Version (100092) **internal** | **recon** | **unauth**	139 / tcp smb	Trivial
LAN Manager: Samba 4.6.2 Domain: SAMBA OS: Windows 6.1		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal** | **explicit** | **unauth**	81 / tcp http (ssl)	Trivial
Server supports TLS version 1.0		

192.168.67.77 B

IP: 192.168.67.77
Asset name: 192.168.67.77
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

DEBIAN B

IP: 192.168.67.78
Asset name: DEBIAN
Operating system: Debian 6 Linux
Asset type: Server

Protocol	Service

ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
http	80 / tcp
rpcbind	111 / tcp
rpcbind	111 / udp
netbios-ns	137 / udp
smb	139 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Web Server Directory Indexing Enabled (101049) **internal | explicit | unauth**	80 / tcp http	Low
Directory Indexing Enabled: 192.168.67.78:80: /icons		
Apache Range Header Denial Of Service (117860) **internal | explicit | unauth**	80 / tcp http	Low
Webserver returned: 206 Partial Content		
Apache Username Disclosure (101469) **internal | explicit | unauth**	80 / tcp http	Low
Apache username disclosure detected: /~root		
Webserver Expect Header Allows Cross-Site Scripting (104910) **internal | explicit | unauth**	80 / tcp http	Low
[Large data section omitted]		

SMB Security Signatures Not Required (104188)
internal | explicit | unauth
139 / tcp
smb
Low

SMBv1 NTLM signatures are not required

Apache Manual Page Information Leak (103390)
internal | explicit | unauth
80 / tcp
http
Low

Apache 1.3 documentation page detected.

Apache Default Start Page (103388)
internal | recon | unauth
80 / tcp
http
Low

Unconfigured Apache server detected

Product Has Reached End-of-Life Status (104220)
internal | explicit | unauth
80 / tcp
http
Low

Version 1.3.24 of the Apache Web Server has reached end-of-life status.

ISC BIND End Of Life (123915)
internal | explicit | unauth
53 / tcp
dns
Low

ISC Bind version 9.7.3 has surpassed its EOL date.

SMB User Enumeration (113348)
internal | explicit | unauth
139 / tcp
smb
Low

Users for domain 'DEBIAN':
nobody
buff

Samba End of Life (117557)
internal | explicit | unauth
139 / tcp
smb
Low

Samba 3.5.6 has reached end-of-life status.

Debian End of Life (134009)
internal | explicit | unauth
22 / tcp
ssh
Low

Debian 6.0 has reached end-of-life status.

ISC BIND End Of Life (123915)
internal | explicit | unauth
53 / udp
dns
Low

ISC Bind version 9.7.3 has surpassed its EOL date.

SMB Null Session Authentication (101373)
internal | recon | unauth
139 / tcp
smb
Trivial

It was possible to log into the remote host using a NULL session.

RPC Portmap Service (100505) — 111 / tcp — Trivial
internal | explicit | unauth — rpcbind

Not Applicable

RPC Portmap Service (100505) — 111 / udp — Trivial
internal | explicit | unauth — rpcbind

Not Applicable

HTTP TRACE/TRACK Method Enabled (117856) — 80 / tcp — Trivial
internal | explicit | unauth — http

Not Applicable

Apache ETags Inode Number Disclosure (121914) — 80 / tcp — Trivial
internal | explicit | unauth — http

The instance of Apache running on this asset at TCP port 80 discloses inode numbers in ETag header fields:

ETag Header Value: 2f44bb-5c3-51756615;51756615
Inode Number: 3097787
File Size: 1475 bytes
Last Modified (Epoch): NaN

SMB Native LanMan Version (100092) — 139 / tcp — Trivial
internal | recon | unauth — smb

LAN Manager: Samba 3.5.6
Domain: WORKGROUP
OS: Unix

192.168.67.79	**B**

IP: 192.168.67.79
Asset name: 192.168.67.79
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.87	B

IP: 192.168.67.87
Asset name: 192.168.67.87
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.90	B

IP: 192.168.67.90
Asset name: 192.168.67.90
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.96	B

IP: 192.168.67.96
Asset name: 192.168.67.96
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.101	B

IP: 192.168.67.101
Asset name: 192.168.67.101
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

S1-WIN2019-SV01	B

IP: 192.168.67.236
Asset name: S1-WIN2019-SV01
Operating system: Windows Server 2019
Asset type: Server

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SMB Security Signatures Not Required (104188) **internal** | **explicit** | **unauth**	139 / tcp netbios	Low
SMBv2 NTLM signatures are not required		
SMB Native LanMan Version (100092) **internal** | **recon** | **unauth**	139 / tcp netbios	Trivial
LAN Manager: 10.0.17763.15 Domain: AD01 OS: Windows 2019 Build 17763		

192.168.68.51	B

IP: 192.168.68.51

Asset name: 192.168.68.51
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.51	B

IP: 192.168.68.51
Asset name: 192.168.68.51
Operating system: unknown
Asset type: Server

Protocol	Service
http	80 / tcp
http (ssl)	443 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Web Server Directory Indexing Enabled (101049) internal | explicit | unauth	80 / tcp http	Low

Directory Indexing Enabled:
192.168.68.51:80:
/bitnami/images

HTTP Host Header Value Reflection (128596)

internal | explicit | unauth

80 / tcp
http

Low

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
ECDHE-RSA-AES256-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

Content Security Policy Missing (148043)

internal | explicit | unauth

80 / tcp
http

Trivial

Missing Content Security Policy.

Content Security Policy Missing (148043)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Missing Content Security Policy.

SSL Certificate: Outdated Version (104020)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Outdated SSL Certificate Version: 1

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

443 / tcp
http (ssl)

Trivial

Server supports TLS version 1.0

192.168.68.56 B

IP: 192.168.68.56
Asset name: 192.168.68.56
Operating system: Linux Variant

Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp
mysql	3306 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Anonymous FTP Enabled (101362) **internal | explicit | unauth**	21 / tcp ftp	Low

anonymous

192.168.68.57	B

IP: 192.168.68.57
Asset name: 192.168.68.57
Operating system: Debian 9 Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Phpinfo.php System Information Disclosure (100403) **internal | explicit | unauth**	80 / tcp http	Low
[Large data section omitted]		
Debian End of Life (134009) **internal | explicit | unauth**	22 / tcp ssh	Low
Debian 9.0 has reached end-of-life status.		
HTTP Host Header Value Reflection (128596) **internal | explicit | unauth**	80 / tcp http	Low
/manual : an't connect to vm.frontline.cloud:80 (Bad hostnam		
Apache Manual Page Information Leak (103390) **internal | explicit | unauth**	80 / tcp http	Low
Apache 2.4 documentation page detected.		
Content Security Policy Missing (148043) **internal | explicit | unauth**	80 / tcp http	Trivial
Missing Content Security Policy.		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		

192.168.68.59 B

IP: 192.168.68.59
Asset name: 192.168.68.59
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Content Security Policy Missing (148043) internal | explicit | unauth	80 / tcp http	Trivial
Missing Content Security Policy.		
Web Server Default Error Page Detected (128223) internal | explicit | unauth	80 / tcp http	Trivial
[Large data section omitted]		

192.168.68.59 B

IP: 192.168.68.59
Asset name: 192.168.68.59
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp
mysql	3306 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Anonymous FTP Enabled (101362) internal | explicit | unauth	21 / tcp ftp	Low
anonymous		

192.168.68.60	B

IP: 192.168.68.60
Asset name: 192.168.68.60
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.62	B

IP: 192.168.68.62
Asset name: 192.168.68.62
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.63	B

IP: 192.168.68.63
Asset name: 192.168.68.63
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.64	B

IP: 192.168.68.64
Asset name: 192.168.68.64
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.64 B

IP: 192.168.68.64
Asset name: 192.168.68.64
Operating system: FreeBSD
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
FreeBSD End of Life (117558) **internal** | **explicit** | **unauth**	N/A / tcp unknown	Low

FreeBSD 11.1 has reached end-of-life status.

192.168.68.67 B

IP: 192.168.68.67
Asset name: 192.168.68.67
Operating system: CentOS
Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp
http	80 / tcp
mysql	3306 / tcp
unknown	N/A / tcp

unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity
Web Server Directory Indexing Enabled (101049) **internal | explicit | unauth**	80 / tcp http	Low
Directory Indexing Enabled: 192.168.68.67:80: /icons /icons/small		
Slowloris Resource Depletion And Denial Of Service (117854) **internal | explicit | unauth**	80 / tcp http	Low
The webserver appears to be vulnerable to a resource exhaustion attack.		
Anonymous FTP Enabled (101362) **internal | explicit | unauth**	21 / tcp ftp	Low
anonymous		
Product Has Reached End-of-Life Status (104220) **internal | explicit | unauth**	80 / tcp http	Low
Version 2.2.15 of the Apache Web Server has reached end-of-life status.		
PHP End of Life (112906) **internal | explicit | unauth**	80 / tcp http	Low
Version 5.3.3 of PHP has reached end-of-life status.		
Apache Default Start Page (103388) **internal | recon | unauth**	80 / tcp http	Low
Unconfigured Apache server detected		
HTTP TRACE/TRACK Method Enabled (117856) **internal | explicit | unauth**	80 / tcp http	Trivial
Not Applicable		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial

[Large data section omitted]

192.168.68.68	B

IP: 192.168.68.68
Asset name: 192.168.68.68
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.68.69	B

IP: 192.168.68.69
Asset name: 192.168.68.69
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	Failure	N/A

Vulnerability Title	Service(s)	Severity

Content Security Policy Missing (148043) **internal | explicit | unauth**	80 / tcp http	Trivial
	Missing Content Security Policy.	
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
	[Large data section omitted]	

192.168.68.86 — B

IP: 192.168.68.86
Asset name: 192.168.68.86
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Ubuntu End of Life (117365) **internal | explicit | unauth**	N/A / tcp unknown	Low
Ubuntu 12.04 has reached end-of-life status.		

UBUNTU-14-SERVE — B

IP: 192.168.68.92
Asset name: UBUNTU-14-SERVE
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp

dns	53 / tcp
dns	53 / udp
http	80 / tcp
pop3	110 / tcp
netbios-ns	137 / udp
smb	139 / tcp
imap	143 / tcp
imap (ssl)	993 / tcp
pop3 (ssl)	995 / tcp
http	8080 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Slowloris Resource Depletion And Denial Of Service (117854) **internal | explicit | unauth**	8080 / tcp http	Low
The webserver appears to be vulnerable to a resource exhaustion attack.		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Low
[Large data section omitted]		
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal | explicit | unauth**	143 / tcp imap	Low
[Large data section omitted]		

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | explicit | unauth

110 / tcp
pop3

Low

[Large data section omitted]

SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343)

internal | explicit | unauth

993 / tcp
imap (ssl)

Low

[Large data section omitted]

SMB Security Signatures Not Required (104188)

internal | explicit | unauth

139 / tcp
smb

Low

SMBv1 NTLM signatures are not required
SMBv2 NTLM signatures are not required

SSL Connection: SSL Version 3 Enabled (128440)

internal | explicit | unauth

995 / tcp
pop3 (ssl)

Low

Server supports SSL version 3

ISC BIND End Of Life (123915)

internal | explicit | unauth

53 / udp
dns

Low

ISC Bind version 9.9.5 has surpassed its EOL date.

ISC BIND End Of Life (123915)

internal | explicit | unauth

53 / tcp
dns

Low

ISC Bind version 9.9.5 has surpassed its EOL date.

SMB User Enumeration (113348)

internal | explicit | unauth

139 / tcp
smb

Low

Users for domain 'UBUNTU-14-SERVER':
buff

SSL Connection: SSL Version 3 Enabled (128440)

internal | explicit | unauth

110 / tcp
pop3

Low

Server supports SSL version 3

SSL Connection: SSL Version 3 Enabled (128440)

internal | explicit | unauth

993 / tcp
imap (ssl)

Low

Server supports SSL version 3

SSL Connection: SSL Version 3 Enabled (128440) **internal | explicit | unauth**	143 / tcp imap	Low
	Server supports SSL version 3	
SMB Null Session Authentication (101373) **internal | recon | unauth**	139 / tcp smb	Trivial
	It was possible to log into the remote host using a NULL session.	
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
	[Large data section omitted]	
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	110 / tcp pop3	Trivial
	[Large data section omitted]	
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	143 / tcp imap	Trivial
	[Large data section omitted]	
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
	[Large data section omitted]	
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
	[Large data section omitted]	
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	143 / tcp imap	Trivial
	[Large data section omitted]	
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	110 / tcp pop3	Trivial
	[Large data section omitted]	
SSL Connection: SSL/TLS Supports RC4 Ciphers (113293) **internal | explicit | unauth**	993 / tcp imap (ssl)	Trivial
	[Large data section omitted]	

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

995 / tcp
pop3 (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

993 / tcp
imap (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

110 / tcp
pop3

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

143 / tcp
imap

Trivial

[Large data section omitted]

Web Server Default Error Page Detected (128223)

internal | **explicit** | **unauth**

80 / tcp
http

Trivial

[Large data section omitted]

Default Apache Tomcat Webpage Detected (117554)

internal | **recon** | **unauth**

8080 / tcp
http

Trivial

Default Apache Tomcat 6 webpage detected

SMB Native LanMan Version (100092)

internal | **recon** | **unauth**

139 / tcp
smb

Trivial

LAN Manager: Samba 4.3.9-Ubuntu
Domain: WORKGROUP
OS: Windows 6.1

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | **explicit** | **unauth**

993 / tcp
imap (ssl)

Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | **explicit** | **unauth**

993 / tcp
imap (ssl)

Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	110 / tcp pop3	Trivial
Server supports TLS version 1.1		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	110 / tcp pop3	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	143 / tcp imap	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	143 / tcp imap	Trivial
Server supports TLS version 1.1		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
Server supports TLS version 1.1		
TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	995 / tcp pop3 (ssl)	Trivial
Server supports TLS version 1.0		

UBUNTU-16-SERVE B

IP: 192.168.68.108
Asset name: UBUNTU-16-SERVE
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
http	80 / tcp
pop3	110 / tcp

netbios-ns	137 / udp
smb	139 / tcp
imap	143 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp smb	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SMB Null Session Authentication (101373) **internal | recon | unauth**	139 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		
SMB Native LanMan Version (100092) **internal | recon | unauth**	139 / tcp smb	Trivial
LAN Manager: Samba 4.3.11-Ubuntu Domain: WORKGROUP OS: Windows 6.1		

192.168.68.111 B

IP: 192.168.68.111
Asset name: 192.168.68.111
Operating system: Linux Variant
Asset type: Server

Protocol	Service

ssh	22 / tcp
http (ssl)	81 / tcp
http	82 / tcp
http (ssl)	83 / tcp
smb	139 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
HTTP Host Header Value Reflection (128596) **internal | explicit | unauth**	81 / tcp http (ssl)	Low
/app/base/session/login/L2FwcC9iYXNlLw__ : action="https://vm.frontline.cloud/app/base/sessio /app/base/session/login/text/ : action="https://vm.frontline.cloud/app/base/sessio		
SSL Connection: SSL Version 3 Enabled (128440) **internal | explicit | unauth**	81 / tcp http (ssl)	Low
Server supports SSL version 3		
SMB User Enumeration (113348) **internal | explicit | unauth**	139 / tcp smb	Low
Users for domain 'CLEAROS': admin		
HTTP Host Header Value Reflection (128596) **internal | explicit | unauth**	82 / tcp http	Low
/app/base/session/login/L2FwcC9iYXNlLw__ : action="http://vm.frontline.cloud/app/base/sessio		
SMB Null Session Authentication (101373) **internal | recon | unauth**	139 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		

SSL Connection: Sweet32 Vulnerability (121110)

internal | **explicit** | **unauth**

83 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Connection: Sweet32 Vulnerability (121110)

internal | **explicit** | **unauth**

81 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | **explicit** | **unauth**

81 / tcp
http (ssl)

Trivial

[Large data section omitted]

Apache Server Header Information Disclosure (123916)

internal | **recon** | **unauth**

83 / tcp
http (ssl)

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (ClearOS) OpenSSL/1.0.2k-fips

Web Server Default Error Page Detected (128223)

internal | **explicit** | **unauth**

83 / tcp
http (ssl)

Trivial

[Large data section omitted]

Apache Server Header Information Disclosure (123916)

internal | **recon** | **unauth**

82 / tcp
http

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (ClearOS) OpenSSL/1.0.2k-fips

Web Server Default Error Page Detected (128223)

internal | **explicit** | **unauth**

82 / tcp
http

Trivial

[Large data section omitted]

SMB Native LanMan Version (100092)

internal | **recon** | **unauth**

139 / tcp
smb

Trivial

LAN Manager: Samba 4.6.2
Domain: SAMBA
OS: Windows 6.1

Apache Server Header Information Disclosure (123916)

internal | **recon** | **unauth**

81 / tcp
http (ssl)

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (ClearOS) OpenSSL/1.0.2k-fips

Web Server Default Error Page Detected (128223) internal | explicit | unauth	81 / tcp http (ssl)	Trivial
	[Large data section omitted]	
TLS Connection: TLS Version 1.1 Enabled (145426) internal | explicit | unauth	83 / tcp http (ssl)	Trivial
	Server supports TLS version 1.1	
TLS Connection: TLS Version 1.1 Enabled (145426) internal | explicit | unauth	81 / tcp http (ssl)	Trivial
	Server supports TLS version 1.1	
TLS Connection: TLS Version 1.0 Enabled (125641) internal | explicit | unauth	81 / tcp http (ssl)	Trivial
	Server supports TLS version 1.0	

192.168.68.114 B

IP: 192.168.68.114
Asset name: 192.168.68.114
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

DEBIAN B

IP: 192.168.68.211
Asset name: DEBIAN
Operating system: Debian 6 Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
http	80 / tcp
rpcbind	111 / tcp
rpcbind	111 / udp
netbios-ns	137 / udp
smb	139 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Web Server Directory Indexing Enabled (101049) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Directory Indexing Enabled: 192.168.68.211:80: /icons		
Apache Range Header Denial Of Service (117860) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Webserver returned: 206 Partial Content		
Apache Username Disclosure (101469) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Apache username disclosure detected: /~root		
Webserver Expect Header Allows Cross-Site Scripting (104910) **internal** | **explicit** | **unauth**	80 / tcp http	Low

[Large data section omitted]		
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp smb	Low
SMBv1 NTLM signatures are not required		
Apache Manual Page Information Leak (103390) **internal | explicit | unauth**	80 / tcp http	Low
Apache 1.3 documentation page detected.		
ISC BIND End Of Life (123915) **internal | explicit | unauth**	53 / udp dns	Low
ISC Bind version 9.7.3 has surpassed its EOL date.		
Samba End of Life (117557) **internal | explicit | unauth**	139 / tcp smb	Low
Samba 3.5.6 has reached end-of-life status.		
SMB User Enumeration (113348) **internal | explicit | unauth**	139 / tcp smb	Low
Users for domain 'DEBIAN': nobody buff		
ISC BIND End Of Life (123915) **internal | explicit | unauth**	53 / tcp dns	Low
ISC Bind version 9.7.3 has surpassed its EOL date.		
Apache Default Start Page (103388) **internal | recon | unauth**	80 / tcp http	Low
Unconfigured Apache server detected		
Product Has Reached End-of-Life Status (104220) **internal | explicit | unauth**	80 / tcp http	Low
Version 1.3.24 of the Apache Web Server has reached end-of-life status.		
Debian End of Life (134009) **internal | explicit | unauth**	22 / tcp ssh	Low
Debian 6.0 has reached end-of-life status.		

RPC Portmap Service (100505)

internal | **explicit** | **unauth**

111 / udp
rpcbind

Trivial

Not Applicable

RPC Portmap Service (100505)

internal | **explicit** | **unauth**

111 / tcp
rpcbind

Trivial

Not Applicable

SMB Null Session Authentication (101373)

internal | **recon** | **unauth**

139 / tcp
smb

Trivial

It was possible to log into the remote host using a NULL session.

HTTP TRACE/TRACK Method Enabled (117856)

internal | **explicit** | **unauth**

80 / tcp
http

Trivial

Not Applicable

Apache ETags Inode Number Disclosure (121914)

internal | **explicit** | **unauth**

80 / tcp
http

Trivial

The instance of Apache running on this asset at TCP port 80 discloses inode numbers in ETag header fields:

ETag Header Value: 2f44bb-5c3-51756615;51756615
Inode Number: 3097787
File Size: 1475 bytes
Last Modified (Epoch): NaN

SMB Native LanMan Version (100092)

internal | **recon** | **unauth**

139 / tcp
smb

Trivial

LAN Manager: Samba 3.5.6
Domain: WORKGROUP
OS: Unix

192.168.69.103 — B

IP: 192.168.69.103
Asset name: 192.168.69.103
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.114 B

IP: 192.168.69.114
Asset name: 192.168.69.114
Operating system: unknown
Asset type: Server

Protocol	Service
http	80 / tcp
http (ssl)	443 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Web Server Directory Indexing Enabled (101049) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Directory Indexing Enabled: 192.168.69.114:80: /bitnami/images		
HTTP Host Header Value Reflection (128596) **internal** | **explicit** | **unauth**	80 / tcp http	Low
[Large data section omitted]		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal** | **explicit** | **unauth**	443 / tcp http (ssl)	Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial

Server supports TLS version 1.0

SSL Certificate: Outdated Version (104020) **internal | explicit | unauth**	443 / tcp http (ssl)	Trivial

Outdated SSL Certificate Version: 1

192.168.69.118 B

IP: 192.168.69.118
Asset name: 192.168.69.118
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp
unknown	68 / udp
ntp	123 / udp
mysql	3306 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Anonymous FTP Enabled (101362) internal | explicit | unauth	21 / tcp ftp	Low
	anonymous	

192.168.69.120	B

IP: 192.168.69.120
Asset name: 192.168.69.120
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.122	B

IP: 192.168.69.122
Asset name: 192.168.69.122
Operating system: CentOS
Asset type: Server

Protocol	Service
ftp	21 / tcp
ssh	22 / tcp
unknown	68 / udp
http	80 / tcp
ntp	123 / udp

mysql	3306 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Web Server Directory Indexing Enabled (101049) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Directory Indexing Enabled: 192.168.69.122:80: /icons /icons/small		
Slowloris Resource Depletion And Denial Of Service (117854) **internal** | **explicit** | **unauth**	80 / tcp http	Low
The webserver appears to be vulnerable to a resource exhaustion attack.		
Apache Username Disclosure (101469) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Apache username disclosure detected: /~root		
Phpinfo.php System Information Disclosure (100403) **internal** | **explicit** | **unauth**	80 / tcp http	Low
[Large data section omitted]		
Anonymous FTP Enabled (101362) **internal** | **explicit** | **unauth**	21 / tcp ftp	Low
anonymous		
Apache Default Start Page (103388) **internal** | **recon** | **unauth**	80 / tcp http	Low
Unconfigured Apache server detected		
Product Has Reached End-of-Life Status (104220) **internal** | **explicit** | **unauth**	80 / tcp http	Low

	Version 2.2.15 of the Apache Web Server has reached end-of-life status.

PHP End of Life (112906) **internal | explicit | unauth**	80 / tcp http	Low
	Version 5.3.3 of PHP has reached end-of-life status.	
HTTP TRACE/TRACK Method Enabled (117856) **internal | explicit | unauth**	80 / tcp http	Trivial
	Not Applicable	
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
	[Large data section omitted]	

WIN-30QQRC10MGG B

IP: 192.168.69.123
Asset name: WIN-30QQRC10MGG
Operating system: Windows Server 2012 R2
Asset type: Server

Protocol	Service
http	80 / tcp
http	83 / tcp
msrpc	135 / tcp
netbios-ns	137 / udp
netbios	139 / tcp
http (ssl)	443 / tcp
msrdp	3389 / tcp
winrm	5985 / tcp
http	47001 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) (121756) **internal** | **explicit** | **unauth**	135 / tcp msrpc	Medium

This asset permits binding to samr pipe using auth level Connect.
Response from asset:
02 .

22 00 00 c0 "...

Responding port: 49153

Vulnerability Title	Service(s)	Severity
Insecure Crossdomain.xml Directives (104181) **internal** | **explicit** | **unauth**	83 / tcp http	Low

```
Path: /crossdomain.xml
Content:
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<cross-domain-policy>
<allow-access-from domain="*" />
</cross-domain-policy>
```

Vulnerability Title	Service(s)	Severity
SSL Connection: Server Vulnerable to Bar Mitzvah Attack (119343) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Low

Vulnerable to Bar Mitzvah attack.
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2

Vulnerability Title	Service(s)	Severity
SSL Connection: Sweet32 Vulnerability (121110) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial

SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack:
TLSv1:
DES-CBC3-SHA

TLSv1.1:
DES-CBC3-SHA

TLSv1.2:
DES-CBC3-SHA

SSL Certificate: Weak Signature Algorithm SHA-1 (121119)

3389 / tcp
msrdp

Trivial

internal | explicit | unauth

Weak Signature Algorithm: SHA-1

SSL Connection: SSL/TLS Supports RC4 Ciphers (113293)

3389 / tcp
msrdp

Trivial

internal | explicit | unauth

```
SSL connection supports the following SSL/TLS RC4 ciphers:
RC4-MD5 - TLSv1
RC4-SHA - TLSv1
RC4-MD5 - TLSv1.1
RC4-SHA - TLSv1.1
RC4-MD5 - TLSv1.2
RC4-SHA - TLSv1.2
```

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

3389 / tcp
msrdp

Trivial

internal | explicit | unauth

```
SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: server ignores client order but prefers CBC mode ciphers
Cipher used: ECDHE-RSA-AES256-SHA
```

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

443 / tcp
http (ssl)

Trivial

internal | explicit | unauth

[Large data section omitted]

SSL Certificate: Outdated Version (104020)

443 / tcp
http (ssl)

Trivial

internal | explicit | unauth

Outdated SSL Certificate Version: 1

TLS Connection: TLS Version 1.0 Enabled (125641)

443 / tcp
http (ssl)

Trivial

internal | explicit | unauth

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426)

443 / tcp
http (ssl)

Trivial

internal | explicit | unauth

Server supports TLS version 1.1

TLS Connection: TLS Version 1.0 Enabled (125641) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
Server supports TLS version 1.0		
TLS Connection: TLS Version 1.1 Enabled (145426) **internal** | **explicit** | **unauth**	3389 / tcp msrdp	Trivial
Server supports TLS version 1.1		
SMB Native LanMan Version (100092) **internal** | **recon** | **unauth**	139 / tcp netbios	Trivial
LAN Manager: 6.3.9600.15 Domain: WIN-30QQRC10MGG OS: Windows 2012 R2 Build 9600		

192.168.69.124 B

IP: 192.168.69.124
Asset name: 192.168.69.124
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.128 B

IP: 192.168.69.128
Asset name: 192.168.69.128
Operating system: unknown
Asset type: Device

Protocol	Service

unknown	68 / udp
ntp	123 / udp
unknown	631 / udp
unknown	5353 / udp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

UBUNTU-16-SERVE	B

IP: 192.168.69.129
Asset name: UBUNTU-16-SERVE
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
dns	53 / tcp
dns	53 / udp
unknown	68 / udp
http	80 / tcp
pop3	110 / tcp
netbios-ns	137 / udp
unknown	138 / udp
smb	139 / tcp

imap	143 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SMB Security Signatures Not Required (104188) **internal | explicit | unauth**	139 / tcp smb	Low
SMBv1 NTLM signatures are not required SMBv2 NTLM signatures are not required		
SMB Null Session Authentication (101373) **internal | recon | unauth**	139 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		
SMB Native LanMan Version (100092) **internal | recon | unauth**	139 / tcp smb	Trivial
LAN Manager: Samba 4.3.11-Ubuntu Domain: WORKGROUP OS: Windows 6.1		
Web Server Default Error Page Detected (128223) **internal | explicit | unauth**	80 / tcp http	Trivial
[Large data section omitted]		

192.168.69.130	**B**

IP: 192.168.69.130
Asset name: 192.168.69.130
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp

unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.131	B

IP: 192.168.69.131
Asset name: 192.168.69.131
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.179	B

IP: 192.168.69.179
Asset name: 192.168.69.179
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
http (ssl)	81 / tcp

http	82 / tcp
http (ssl)	83 / tcp
smb	139 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
HTTP Host Header Value Reflection (128596) **internal | explicit | unauth**	81 / tcp http (ssl)	Low
/app/base/session/login/ : action="https://vm.frontline.cloud/app/base/sessio /app/base/session/login/L2FwcC9iYXNlLw__ : action="https://vm.frontline.cloud/app/base/sessio		
SSL Connection: SSL Version 3 Enabled (128440) **internal | explicit | unauth**	81 / tcp http (ssl)	Low
Server supports SSL version 3		
SMB User Enumeration (113348) **internal | explicit | unauth**	139 / tcp smb	Low
Users for domain 'CLEAROS': admin		
HTTP Host Header Value Reflection (128596) **internal | explicit | unauth**	82 / tcp http	Low
/app/base/session/login/L2FwcC9iYXNlLw__ : action="http://vm.frontline.cloud/app/base/sessio		
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	83 / tcp http (ssl)	Trivial
[Large data section omitted]		
SMB Null Session Authentication (101373) **internal | recon | unauth**	139 / tcp smb	Trivial
It was possible to log into the remote host using a NULL session.		

SSL Connection: Sweet32 Vulnerability (121110)

internal | explicit | unauth

81 / tcp
http (ssl)

Trivial

[Large data section omitted]

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276)

internal | explicit | unauth

81 / tcp
http (ssl)

Trivial

[Large data section omitted]

TLS Connection: TLS Version 1.0 Enabled (125641)

internal | explicit | unauth

81 / tcp
http (ssl)

Trivial

Server supports TLS version 1.0

Web Server Default Error Page Detected (128223)

internal | explicit | unauth

81 / tcp
http (ssl)

Trivial

[Large data section omitted]

Apache Server Header Information Disclosure (123916)

internal | recon | unauth

81 / tcp
http (ssl)

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (ClearOS) OpenSSL/1.0.2k-fips

TLS Connection: TLS Version 1.1 Enabled (145426)

internal | explicit | unauth

81 / tcp
http (ssl)

Trivial

Server supports TLS version 1.1

SMB Native LanMan Version (100092)

internal | recon | unauth

139 / tcp
smb

Trivial

LAN Manager: Samba 4.6.2
Domain: SAMBA
OS: Windows 6.1

Web Server Default Error Page Detected (128223)

internal | explicit | unauth

83 / tcp
http (ssl)

Trivial

[Large data section omitted]

Apache Server Header Information Disclosure (123916)

internal | recon | unauth

83 / tcp
http (ssl)

Trivial

This instance of Apache discloses version information via the HTTP Server header:
Server: Apache/2.4.6 (ClearOS) OpenSSL/1.0.2k-fips

TLS Connection: TLS Version 1.1 Enabled (145426) internal | explicit | unauth	83 / tcp http (ssl)	Trivial
Server supports TLS version 1.1		
Web Server Default Error Page Detected (128223) internal | explicit | unauth	82 / tcp http	Trivial
[Large data section omitted]		
Apache Server Header Information Disclosure (123916) internal | recon | unauth	82 / tcp http	Trivial
This instance of Apache discloses version information via the HTTP Server header: Server: Apache/2.4.6 (ClearOS) OpenSSL/1.0.2k-fips		

192.168.69.243 — B

IP: 192.168.69.243
Asset name: 192.168.69.243
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
ssh	22 / tcp
http (ssl)	8834 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.100.23 — B

IP: 192.168.100.23
Asset name: 192.168.100.23
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
http	80 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Web Server Directory Indexing Enabled (101049) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Directory Indexing Enabled: 192.168.100.23:80: /css /js		
Product Has Reached End-of-Life Status (104220) **internal** | **explicit** | **unauth**	80 / tcp http	Low
Version 2.2.21 of the Apache Web Server has reached end-of-life status.		
HTTP TRACE/TRACK Method Enabled (117856) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial
Not Applicable		
Apache ETags Inode Number Disclosure (121914) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial
The instance of Apache running on this asset at TCP port 80 discloses inode numbers in ETag header fields: ETag Header Value: 206e-6a8-503e0d1bdfc80 Inode Number: 8302 File Size: 1704 bytes Last Modified (Epoch): 1411639010000000		
Content Security Policy Missing (148043) **internal** | **explicit** | **unauth**	80 / tcp http	Trivial
Missing Content Security Policy.		

Web Server Default Error Page Detected (128223) internal | explicit | unauth	80 / tcp http	Trivial

[Large data section omitted]

10.1.1.20	A

IP: 10.1.1.20
Asset name: 10.1.1.20
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

10.1.1.28	A

IP: 10.1.1.28
Asset name: 10.1.1.28
Operating system: Linux Variant
Asset type: Client

Protocol	Service
ssh	22 / tcp
http	80 / tcp
smb	445 / tcp
http (ssl)	2443 / tcp
http	8000 / tcp

http (ssl)	8001 / tcp
unknown (ssl)	8009 / tcp
ssh	8022 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Content Security Policy Missing (148043) internal | explicit | unauth	80 / tcp http	Trivial
Missing Content Security Policy.		
SSL Certificate: Outdated Version (104020) internal | explicit | unauth	2443 / tcp http (ssl)	Trivial
Outdated SSL Certificate Version: 1		
SMB Native LanMan Version (100092) internal | recon | unauth	445 / tcp smb	Trivial
LAN Manager: 6.1.0.15 Domain: PI3-2 OS: Windows 7 Build 0		

LOCALHOST A

IP: 10.1.1.29
Asset name: LOCALHOST
Operating system: Linux Variant
Asset type: Server

Protocol	Service
ssh	22 / tcp
smtp	25 / tcp
unknown	N/A / tcp

unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

PI3-4	A

IP: 10.1.1.30
Asset name: PI3-4
Operating system: Linux Variant
Asset type: Client

Protocol	Service
ssh	22 / tcp
http	80 / tcp
netbios-ns	137 / udp
smb	139 / tcp
unknown	161 / udp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
Content Security Policy Missing (148043) **internal | explicit | unauth**	80 / tcp http	Trivial
Missing Content Security Policy.		

SMB Native LanMan Version (100092) internal | recon | unauth	139 / tcp smb	Trivial

LAN Manager: 6.1.0.15
Domain: PI3-4
OS: Windows 7 Build 0

tplinkwifi.net A

IP: 192.168.0.1
Asset name: tplinkwifi.net
Operating system: unknown
Asset type: Server

Protocol	Service
unknown (ssl)	443 / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.0.11 A

IP: 192.168.0.11
Asset name: 192.168.0.11
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.0.15	A

IP: 192.168.0.15
Asset name: 192.168.0.15
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.0.111	A

IP: 192.168.0.111
Asset name: 192.168.0.111
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.0.125	A

IP: 192.168.0.125
Asset name: 192.168.0.125
Operating system: unknown
Asset type: Unknown

Protocol	Service

unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.0.143	A

IP: 192.168.0.143
Asset name: 192.168.0.143
Operating system: unknown
Asset type: Device

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.0.172	A

IP: 192.168.0.172
Asset name: 192.168.0.172
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.0.172	A

IP: 192.168.0.172
Asset name: 192.168.0.172
Operating system: unknown
Asset type: Unknown

Protocol	Service
http	8008 / tcp
unknown (ssl)	8009 / tcp
http (ssl)	8443 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Sweet32 Vulnerability (121110) **internal | explicit | unauth**	8009 / tcp unknown (ssl)	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1: DES-CBC3-SHA TLSv1.1: DES-CBC3-SHA TLSv1.2: DES-CBC3-SHA		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) **internal | explicit | unauth**	8009 / tcp unknown (ssl)	Trivial

SSL connection supports the following SSLv3/TLSv1 CBC mode cipher:
AES128-SHA - TLSv1
AES256-SHA - TLSv1
DES-CBC3-SHA - TLSv1
ECDHE-RSA-AES128-SHA - TLSv1
ECDHE-RSA-AES256-SHA - TLSv1

BEAST not mitigated: all supported ciphers are CBC mode ciphers

TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	8009 / tcp unknown (ssl)	Trivial

Server supports TLS version 1.0

TLS Connection: TLS Version 1.1 Enabled (145426) **internal | explicit | unauth**	8009 / tcp unknown (ssl)	Trivial

Server supports TLS version 1.1

192.168.0.193 A

IP: 192.168.0.193
Asset name: 192.168.0.193
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.0.240 A

IP: 192.168.0.240
Asset name: 192.168.0.240
Operating system: unknown
Asset type: Server

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.0.255	A

IP: 192.168.0.255
Asset name: 192.168.0.255
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	161 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

setup.lan	A

IP: 192.168.1.1
Asset name: setup.lan
Operating system: unknown
Asset type: Server

Protocol	Service
http	80 / tcp
http (ssl)	443 / tcp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.1.38	A

IP: 192.168.1.38
Asset name: 192.168.1.38
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.1.39	A

IP: 192.168.1.39
Asset name: 192.168.1.39
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.1.51	A

IP: 192.168.1.51
Asset name: 192.168.1.51
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

John-s-S21-FE.lan	A

IP: 192.168.1.108
Asset name: John-s-S21-FE.lan
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.1.127	A

IP: 192.168.1.127
Asset name: 192.168.1.127
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

OnePlus-Nord-N200-5G.lan	A

IP: 192.168.1.128
Asset name: OnePlus-Nord-N200-5G.lan
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

HSATP-G4M5LN3.lan	A

IP: 192.168.1.137
Asset name: HSATP-G4M5LN3.lan
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.1.156	A

IP: 192.168.1.156
Asset name: 192.168.1.156
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.1.167	A

IP: 192.168.1.167
Asset name: 192.168.1.167
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

Samsung.lan	A

IP: 192.168.1.184
Asset name: Samsung.lan
Operating system: unknown
Asset type: Device

Protocol	Service
http	8080 / tcp
http	8187 / tcp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.1.186	A

IP: 192.168.1.186
Asset name: 192.168.1.186
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

Elizabeth-s-Galaxy-Note20-5G.lan	A

IP: 192.168.1.193
Asset name: Elizabeth-s-Galaxy-Note20-5G.lan

Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

RE220.lan	A

IP: 192.168.1.206
Asset name: RE220.lan
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.1.230	A

IP: 192.168.1.230
Asset name: 192.168.1.230
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

Meross_Smart_Garage.lan	A

IP: 192.168.1.240
Asset name: Meross_Smart_Garage.lan
Operating system: unknown
Asset type: Device

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.51	A

IP: 192.168.67.51
Asset name: 192.168.67.51
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.67.58	A

IP: 192.168.67.58
Asset name: 192.168.67.58
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.67.62	A

IP: 192.168.67.62
Asset name: 192.168.67.62
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.67.63	A

IP: 192.168.67.63
Asset name: 192.168.67.63
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.65	A

IP: 192.168.67.65
Asset name: 192.168.67.65
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.73	A

IP: 192.168.67.73
Asset name: 192.168.67.73
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

WIN8-1-PATCHED A

IP: 192.168.67.83
Asset name: WIN8-1-PATCHED
Operating system: Windows 8.1
Asset type: Client

Protocol	Service
msrpc	135 / tcp
unknown	139 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SMB Native LanMan Version (100092) internal | recon | unauth	139 / tcp unknown	Trivial

LAN Manager: 6.3.9600.15
Domain: QA0
OS: Windows 8.1 Build 9600

DIAZ-PCI A

IP: 192.168.67.84
Asset name: DIAZ-PCI
Operating system: Windows Platform
Asset type: Client

Protocol	Service
msrpc	135 / tcp

netbios-ns	137 / udp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.84	A

IP: 192.168.67.84
Asset name: 192.168.67.84
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.91	A

IP: 192.168.67.91
Asset name: 192.168.67.91
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan

	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.95	A

IP: 192.168.67.95
Asset name: 192.168.67.95
Operating system: unknown
Asset type: Server

Protocol	Service
http	80 / tcp
http (ssl)	443 / tcp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) internal | explicit | unauth	443 / tcp http (ssl)	Trivial
SSL connection supports the following SSLv3/TLSv1 CBC mode cipher: ECDHE-RSA-AES128-SHA - TLSv1 ECDHE-RSA-AES256-SHA - TLSv1 BEAST not mitigated: all supported ciphers are CBC mode ciphers		
TLS Connection: TLS Version 1.0 Enabled (125641) internal | explicit | unauth	443 / tcp http (ssl)	Trivial
Server supports TLS version 1.0		
SSL Certificate: Outdated Version (104020) internal | explicit | unauth	443 / tcp http (ssl)	Trivial

	Outdated SSL Certificate Version: 1

192.168.67.102	A

IP: 192.168.67.102
Asset name: 192.168.67.102
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.119	A

IP: 192.168.67.119
Asset name: 192.168.67.119
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.139	A

IP: 192.168.67.139
Asset name: 192.168.67.139
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.157 A

IP: 192.168.67.157
Asset name: 192.168.67.157
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.194 A

IP: 192.168.67.194
Asset name: 192.168.67.194
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.233	A

IP: 192.168.67.233
Asset name: 192.168.67.233
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.67.234	A

IP: 192.168.67.234
Asset name: 192.168.67.234
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

DIAZ-PCI	A

IP: 192.168.68.53
Asset name: DIAZ-PCI
Operating system: Windows Platform

Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.54	A

IP: 192.168.68.54
Asset name: 192.168.68.54
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.75	A

IP: 192.168.68.75
Asset name: 192.168.68.75
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.76	A

IP: 192.168.68.76
Asset name: 192.168.68.76
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

WIN8-1-PATCHED	A

IP: 192.168.68.99
Asset name: WIN8-1-PATCHED
Operating system: Windows 8.1
Asset type: Client

Protocol	Service
msrpc	135 / tcp
unknown	139 / tcp
unknown	N/A / tcp

unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SMB Native LanMan Version (100092) internal | recon | unauth	139 / tcp unknown	Trivial

```
LAN Manager: 6.3.9600.15
Domain: QA0
OS: Windows 8.1 Build 9600
```

192.168.68.121 A

IP: 192.168.68.121
Asset name: 192.168.68.121
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.68.138 A

IP: 192.168.68.138
Asset name: 192.168.68.138
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.157	A

IP: 192.168.68.157
Asset name: 192.168.68.157
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.160	A

IP: 192.168.68.160
Asset name: 192.168.68.160
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.68.165	A

IP: 192.168.68.165
Asset name: 192.168.68.165
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.68.185	A

IP: 192.168.68.185
Asset name: 192.168.68.185
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.68.219	A

IP: 192.168.68.219
Asset name: 192.168.68.219
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.238	A

IP: 192.168.68.238
Asset name: 192.168.68.238
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.248	A

IP: 192.168.68.248
Asset name: 192.168.68.248
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.68.254	A

IP: 192.168.68.254
Asset name: 192.168.68.254
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.6	A

IP: 192.168.69.6
Asset name: 192.168.69.6
Operating system: unknown
Asset type: Server

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.55	A

IP: 192.168.69.55
Asset name: 192.168.69.55
Operating system: Windows Server 2012 R2 Standard
Asset type: Server

Protocol	Service
unknown	123 / udp
unknown	137 / udp
unknown	138 / udp
unknown	161 / udp
smb	445 / tcp
unknown	500 / udp
lpd	515 / tcp
unknown	4500 / udp
unknown	49152 / tcp
dcerpc	49153 / tcp
dcerpc	49154 / tcp
dcerpc	49155 / tcp
dcerpc	49156 / tcp
dcerpc	49157 / tcp
dcerpc	49158 / tcp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.56	A

IP: 192.168.69.56
Asset name: 192.168.69.56
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	68 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.57	A

IP: 192.168.69.57
Asset name: 192.168.69.57
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	68 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.60	A

IP: 192.168.69.60
Asset name: 192.168.69.60

Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	68 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.69.61	A

IP: 192.168.69.61
Asset name: 192.168.69.61
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	68 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity

No vulnerabilities were identified on this asset.

192.168.69.62	A

IP: 192.168.69.62
Asset name: 192.168.69.62
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	68 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.63	A

IP: 192.168.69.63
Asset name: 192.168.69.63
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	68 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.64	A

IP: 192.168.69.64
Asset name: 192.168.69.64
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	68 / udp

unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.67	A

IP: 192.168.69.67
Asset name: 192.168.69.67
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	68 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.68	A

IP: 192.168.69.68
Asset name: 192.168.69.68
Operating system: Windows Server 2012 R2 Standard
Asset type: Server

Protocol	Service
smb	445 / tcp
unknown	49152 / tcp
dcerpc	49153 / tcp

dcerpc	49154 / tcp
dcerpc	49155 / tcp
dcerpc	49156 / tcp
dcerpc	49157 / tcp
dcerpc	49158 / tcp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.70	A

IP: 192.168.69.70
Asset name: 192.168.69.70
Operating system: Ubuntu Linux
Asset type: Server

Protocol	Service
unknown	68 / udp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.73	A

IP: 192.168.69.73
Asset name: 192.168.69.73
Operating system: unknown

Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.81	A

IP: 192.168.69.81
Asset name: 192.168.69.81
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.105	A

IP: 192.168.69.105
Asset name: 192.168.69.105
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.127 A

IP: 192.168.69.127
Asset name: 192.168.69.127
Operating system: unknown
Asset type: Unknown

Protocol	Service

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

DIAZ-PCI A

IP: 192.168.69.199
Asset name: DIAZ-PCI
Operating system: Windows Platform
Asset type: Client

Protocol	Service
msrpc	135 / tcp
netbios-ns	137 / udp
unknown	N/A / tcp
unknown	N/A / icmp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.69.214	A

IP: 192.168.69.214
Asset name: 192.168.69.214
Operating system: unknown
Asset type: Unknown

Protocol	Service
msrdp	3389 / tcp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Connection: Sweet32 Vulnerability (121110) internal | explicit | unauth	3389 / tcp msrdp	Trivial
SSL Connection Vulnerable To Sweet32 Block Cipher Collision Attack: TLSv1.1: DES-CBC3-SHA TLSv1.2: DES-CBC3-SHA TLSv1: DES-CBC3-SHA		
SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers (112276) internal | explicit | unauth	3389 / tcp msrdp	Trivial
SSL connection supports the following SSLv3/TLSv1 CBC mode cipher: AES128-SHA - TLSv1 AES256-SHA - TLSv1 DES-CBC3-SHA - TLSv1 ECDHE-RSA-AES128-SHA - TLSv1 ECDHE-RSA-AES256-SHA - TLSv1 BEAST not mitigated: all supported ciphers are CBC mode ciphers		

TLS Connection: TLS Version 1.0 Enabled (125641) **internal | explicit | unauth**	3389 / tcp msrdp	Trivial

Server supports TLS version 1.0

192.168.69.215 A

IP: 192.168.69.215
Asset name: 192.168.69.215
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.86.25 A

IP: 192.168.86.25
Asset name: 192.168.86.25
Operating system: unknown
Asset type: Device

Protocol	Service
unknown (ssl)	443 / tcp
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
SSL Certificate: Expired Certificate Date (103615) **internal | explicit | unauth**	443 / tcp unknown (ssl)	Trivial

	Date Appears Invalid: Aug 22 12:36:14 2020 GMT to Aug 22 12:36:14 2021 GMT

192.168.86.250	A

IP: 192.168.86.250
Asset name: 192.168.86.250
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

192.168.100.25	A

IP: 192.168.100.25
Asset name: 192.168.100.25
Operating system: unknown
Asset type: Unknown

Protocol	Service
unknown	N/A / tcp

Authenticated Scan Status	OS	DB	CIS	Threatscan
	N/A	N/A	N/A	N/A

Vulnerability Title	Service(s)	Severity
No vulnerabilities were identified on this asset.		

7 Recommendations for Improving Security

Security is an ongoing process. Implementing some relatively simple practices can improve Demo Account’s security in the long run, and reduce risks in the face of continually changing threats and dynamic network environments. Based on the vulnerabilities outlined in this report, Fortra's Digital Defense recommends that Demo Account implement the following security practices where necessary.

7.1 General Recommendations

The recommendations in this section are general practices that are an essential part of any ongoing security program. Iterating over these items on a regular basis will improve the overall security posture of any network.

7.1.1 Apply Security Patches

Software vendors produce security patches and software updates as new vulnerabilities are discovered, and normally make them available on web sites. Some vendors provide notifications when security patches are made available. Network administrators should apply these security patches as soon as they are made available to ensure their systems are as secure as possible. The administrators should also subscribe to security mailing lists and watch for new vulnerabilities of the operating systems and applications for which they are responsible.

7.1.2 Disable Unnecessary Services

Most operating systems come with a robust collection of network services installed and enabled out of the box. However, most users rely on less than a handful of these services to conduct their day-to-day business. Unused and unnecessary network services can provide an attacker with valuable information about the systems, and possibly a way around your carefully designed security architecture. If a service is not being used, disable it or limit access to it with a firewall or other software, such as TCP-wrappers. Fortra's Digital Defense can assist in deciding which services are necessary and which can be safely disabled.

7.1.3 Improve System Configuration

Many operating systems and applications can be made more secure by preforming a few simple configuration changes. These changes range from disabling default accounts or changing their passwords to disabling vulnerable features and replacing them with more secure ones. The Detailed Report has a vulnerability solution section for the discovered vulnerabilities that provides detailed instructions for necessary configuration changes. Fortra's Digital Defense can assist with these changes if you so desire.

7.1.4 Third Party Security Solutions

The security posture could be enhanced by the use of third part security solutions, such as firewalls, intrusion detection systems, strong authentication, virtual private networks, or configuration management software.

Appendix A

A.1 Report Options and Filters

The following options and filter sets were applied to the original dataset selected by this report. Filters allow the report scope to be narrowed to a selected set of assets and/or vulnerabilities to provide for more actionable data. Only those assets and vulnerabilities selected by the filter set are considered for the information presented in this report.

A.1.1 General Options

Name	Value
Show TOC Page	Yes
Show Purpose Page	Yes
Show Notes	Yes
Show Services On Asset Details	Yes
Show Sitemaps On Web App Details	No
Include Hidden	No
Include Info Vulns	No
Include Acceptable Risk Vulns	Yes
Include Fixed Vulns	No
Active View Window	730 day window
Active View Window Source Date	None
Active View Window Back Days	None days
SLA Days	None days
Exclude SLA Vulnerabilities	No
Data Using Custom Filters	No
Use Active Risk	No
Use Above Threashold Only	No
Use Exploitable Only	No

Name	Value
Trending Number of Intervals	12 intervals
Trending Interval Increment	1
Trending Interval Increment Type	months
Trending Preserve Date	No
Use Dynamic Rating	No
Show Filters Appendix	Yes
Show Ratings Appendix	Yes
Show Scan Settings Appendix	No
Show Vulnerability Dictionary Appendix	Yes

A.1.2 Custom Filters

Name	Operator	Value

No filters applied.

Appendix B

B.1 Evaluation Process

The following paragraphs describe Frontline's vulnerability and security posture rating system.

B.1.1 Vulnerability Severity Definitions

Vulnerabilities are known or unknown defects that can be found in an asset's hardware, software, or configuration. Attackers exploit vulnerabilities to gain access or acquire information from target assets. There is a severity level associated with each vulnerability, which is based on the impact and attack would have on an asset's confidentiality, integrity, and availability.

B.1.1.1 Frontline Severity Levels

Critical	If exploited, an attacker will gain complete control of the asset. Critical-level vulnerabilities are known to have publicly accessible exploits which require little to no expert knowledge to use. In some cases, the presence of critical-level vulnerabilities indicate that the asset has already been compromised. Immediate action must be taken to resolve these vulnerabilities.
High	If exploited, an attacker could gain user or administrative access to the asset and be able to run commands, access or delete files, and launch attacks against other assets. High-level vulnerabilities often require some expert knowledge to exploit and publicly accessible exploits may not be available. These vulnerabilities should be resolved as soon as possible.
Medium	If exploited, an attacker would gain valuable information about the asset, which would aid in gaining access. In many cases, medium-level vulnerabilities are a result of improperly configured services, weak or absent security configurations, or unprotected limited access accounts. These vulnerabilities should be dealt with reasonably quickly.
Low	If exploited, an attacker could gain information about the asset but it would not necessarily lead to access. Low-level vulnerabilities can usually be addressed by applying security hardening practices or disabling services.
Trivial	If exploited, an attacker could gain information about the asset but it should not lead to access. In many cases trivial-level vulnerabilities have no possible solution due to operating system limitations, and pose a minimal risk to the asset's security.
Info	Information provided by an asset or a service that is not considered a vulnerability.

B.1.2 Asset Ratings

Each asset is assigned an asset rating based on the severity of the vulnerabilities it exhibits. These ratings are calculated by identifying the highest severity vulnerabilities on the asset, and then choosing the corresponding asset rating.

B.1.2.1 FVM Rating Levels

F	The asset has one or more critical-level vulnerabilities.
D	The asset has one or more high-level vulnerabilities.
C	The asset has one or more medium-level vulnerabilities.
B	The asset has one or more low-level vulnerabilities.
A	The asset has zero or more trivial-level vulnerabilities.

B.2 Overall Rating Definitions

The overall rating is based on the average rating values of each asset in the report.

B.2.1 Frontline's Security GPA

F	The weighted average asset Security GPA is 0.00 - 0.33.
D-	The weighted average asset Security GPA is 0.34 - 0.67.
D	The weighted average asset Security GPA is 0.68 - 1.00.
D+	The weighted average asset Security GPA is 1.01 - 1.33.
C-	The weighted average asset Security GPA is 1.34 - 1.67.
C	The weighted average asset Security GPA is 1.68 - 2.00.
C+	The weighted average asset Security GPA is 2.01 - 2.33.
B-	The weighted average asset Security GPA is 2.34 - 2.67.
B	The weighted average asset Security GPA is 2.68 - 3.00.
B+	The weighted average asset Security GPA is 3.01 - 3.33.

A-	The weighted average asset Security GPA is 3.34 - 3.67.
A	The weighted average asset Security GPA is 3.68 - 4.00.

Appendix C

C.1 Vulnerability Dictionary

The following paragraphs describe the reports vulnerabilities in detail.

Easily Guessable SSH Credentials — Critical

Solution Details

It is advised that the password of the account(s) listed in the data section be changed to something secure and complex.

Vulnerability Details

The SSH Server on the remote host has accounts configured with default or weak passwords. Attackers can easily leverage this condition to gain complete access to this host.

False Positive Notes

This item is not likely to be a false positive. However, it's possible that the credentials are valid but yield no usable shell access. The scanner is looking at the response from the SSH service that indicates the credentials are valid, it does not validate that a usable shell is available. This is done because the check needs to work on a wide variety of devices that run many different shells with no consistent functionality to use to validate access.

If it is determined that no usable functionality is accessible using the detected credentials, and it's not possible to change them or disable the service, this can be marked as a false positive.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0502
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0505
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0501
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0507
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0503

Emerson Avocent Default SSH Credentials — Critical

Solution Details

Change the default password for the "admin" account to something complex, preferably alphanumeric with special characters.

Vulnerability Details

This asset appears to be an Emerson Avocent device that is using the default credentials of admin/avocent.
Impact:
An attacker would be able to remotely administer this device utilizing the default credentials.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
There are no references for this vulnerability.	

HTTP Easily Guessable Credentials — Critical

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

It is advised that the password of the account(s) listed in the data section be changed to something secure and complex.

Vulnerability Details

The web application on this host has accounts configured with default or weak passwords. Attackers can easily leverage this condition to gain complete access to the web application.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
There are no references for this vulnerability.	

MS08-067 Microsoft Windows Server Service Stack Overflow (Network Check) — Critical

Solution Details

Hosts connected to the Internet should have a minimal number of ports exposed. Microsoft has released a security bulletin to address this issue. Please obtain and apply the appropriate upgrade as described in the MS08-067 Security Bulletin linked in the References List of the vulnerability details.

Workarounds include;
Disabling the Computer Browser and Server service, but services dependent on the Computer Browser service may log an error message in the system event log. If the Server service is disabled, files or printers cannot be shared from this host, but file shares and printer resources on other hosts will still be available.
Hosts running Windows Vista and Windows Server 2008 can be configured to selectively filter RPC Universally Unique Identifiers (UUID).
Blocking TCP ports 139 and 445 at the firewall will help protect hosts located behind the firewall. It is recommended that all unsolicited inbound communication from the Internet be blocked.

Vulnerability Details

This host is running a version of Windows vulnerable to a code execution flaw within the Microsoft Windows Server Service. The netapi32.dll 'NetrpPathCanonicalize' function contains a stack overflow flaw. Remote attackers can leverage this flaw using a crafted RPC request through Windows SMB/DCERPC to trigger a buffer overflow and execute arbitrary code with SYSTEM privileges, or cause a denial of service. This vulnerability is being actively exploited in the wild (including trojan Gimmiv and NAVI worm).

Note: On some operating systems Windows Update will report MS12-054 as the preferred patch for this vector. Installing that patch will remediate this issue as well.

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4250
BUGTRAQ	http://www.securityfocus.com/bid/31874
URL	https://cwe.mitre.org/data/definitions/94.html
URL	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067
URL	http://blogs.securiteam.com/index.php/archives/1150

MS09-050 Microsoft Windows SMB2 Command Execution Vulnerabilities (Network Check)

Critical

Solution Details

Microsoft has released updates to address this issue. If automatic updating is not enabled, please obtain the appropriate update from the Microsoft Update service, linked in the References List of the vulnerability details. Alternatively, several workarounds are available: either restrict access to TCP ports 139 and 445, or disable SMB v2.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This host is running Microsoft Windows. The SMB2 protocol implementation in the srv2.sys kernel driver contains an array indexing error. Additionally, a flaw exists in the processing of SMBv2 packets and SMB command values. An attacker can leverage a specifically crafted SMB or SMBv2 packet to dereference out-of-bounds memory or trigger in an infinite loop, both resulting in an arbitrary code execution. Failed exploits will result in a DoS condition.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-3103
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2526
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2532
BUGTRAQ	http://www.securityfocus.com/bid/36299
URL	http://www.reversemode.com/index.php?option=com_content&task=view&id=64&Itemid=1
URL	http://g-laurent.blogspot.com/2009/09/windows-vista7-smb20-negotiate-protocol.html
URL	http://isc.sans.org/diary.html?storyid=7093
URL	http://blog.48bits.com/?p=510
URL	https://cwe.mitre.org/data/definitions/94.html
URL	https://cwe.mitre.org/data/definitions/399.html

MS17-010: SMB Remote Code Execution Vulnerability (Network Check) — Critical

Solution Details

Microsoft originally released a fix for these flaws in their March 2017 Quality Update. If this asset is running a supported operating system, please download and install the most recent month's rollup update from the Microsoft Update Catalog or run Windows Update on the affected asset.

If this asset is running Windows XP, Windows Server 2003 or Windows 8, which are no longer supported by Microsoft, Microsoft released patches for these operating systems in the wake of the "WannaCrypt" ransomware attack. The patches for these versions of Windows can be downloaded from the links included in Microsoft's blog post about the "WannaCrypt" ransomware attack, which is linked in the external references section of this vulnerability description. Alternatively, they can be downloaded from the Microsoft Update Catalog link, which is also in the external references section of this vulnerability description.
Workarounds:
If applying the update is not feasible, the risk can be mitigated by disabling the affected service.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This asset is missing the MS17-010 patch, which addresses multiple security vulnerabilities, including remotely exploitable SMB vulnerabilities. Additionally, this patch fixes the vulnerabilities used by the "EternalBlue", "EternalChampion", "EternalRomance", and "EternalSynergy" exploits that were leaked by the Shadow Brokers.
Impact:
A remote, unauthenticated attacker could leverage these vulnerabilities to gain privileged access to this asset. Exploits for these vulnerabilities are publicly available.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0148
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0143
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0147
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0144
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0146
BUGTRAQ	http://www.securityfocus.com/bid/96709
BUGTRAQ	http://www.securityfocus.com/bid/96706
BUGTRAQ	http://www.securityfocus.com/bid/96703
BUGTRAQ	http://www.securityfocus.com/bid/96704
BUGTRAQ	http://www.securityfocus.com/bid/96707

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/96705
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf
URL	https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0148
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144
URL	https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0146
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0145
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0147

MS19-MAY: Microsoft RDP 'BlueKeep' Unauthenticated Remote Code Execution (Network Check) — Critical

Solution Details

Microsoft has released an update to address this vulnerability.

Depending on your operating system, this update may need to be obtained and installed manually from the vendors website.

Note:
It's been observed that in some cases the Microsoft patch doesn't appear to fully apply to remediate the vulnerability. Please verify your version of \windows\system32\drivers\termdd.sys against the version in the File Information section of the appropriate Microsoft KB article that matches your version of Windows.

List of relevant KBs can be found via the External References section from microsoft.com.
Workarounds:
This vulnerability can be mitigated, to a degree, by enabling Network Level Authentication (NLA), however, the affected asset would still be vulnerable to attackers who possess valid credentials.

Disabling RDP completely mitigates this vulnerability.

Vulnerability Details

A vulnerability affecting multiple versions of Windows exists in Microsoft Remote Desktop Services (Terminal Services), which would allow a remote, unauthenticated attacker to leverage a heap corruption, by sending specially crafted packets, to execute arbitrary code, or create a Denial of Service (DoS) condition.
Impact:
A remote, unauthenticated attacker could leverage this vulnerability to execute arbitrary code in kernel address space, effectively gaining SYSTEM level privileges, or cause a Denial of Service condition.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0708
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
URL	http://www.huawei.com/en/psirt/security-notices/huawei-sn-20190515-01-windows-en
URL	https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-433987.pdf
URL	http://packetstormsecurity.com/files/153627/Microsoft-Windows-RDP-BlueKeep-Denial-Of-Service.html
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-166360.pdf

Type	Reference
URL	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190529-01-windows-en
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-932041.pdf
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-616199.pdf
URL	http://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Desktop-BlueKeep-Denial-Of-Service.html
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-832947.pdf
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-406175.pdf

Samba IsKnownPipename Remote Code Execution — Critical

Solution Details

Update to the latest version of Samba, or apply patches provided by the vendor.
Caveats:
Disabling NT pipe support in Samba can result in degraded functionality for Windows clients.
Workarounds:
If updating and patching are not feasible, the following workaround can be used to mitigate this vulnerability:

Add the following line to the [global] section of the smb.conf Samba configuration file

nt pipe support = no

Vulnerability Details

Samba versions 3.5.0 through 4.6.4/4.5.10/4.4.14, excluding versions in between the last three, are vulnerable to a remote code execution vulnerability resulting from the loading of untrusted libraries during a named pipe connection.
Impact:
A remote, authenticated attacker, or an unauthenticated attacker in cases where an anonymous share contains a writeable directory, can leverage this vulnerability by uploading a payload packaged as an elf so library to a writeable share, and establishing a named pipe connection to the path of the payload, causing Samba to execute the library. Successful exploitation of this vulnerability would result in a complete compromise of the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7494
BUGTRAQ	http://www.securityfocus.com/bid/98636
URL	https://www.samba.org/samba/security/CVE-2017-7494.html
URL	https://cwe.mitre.org/data/definitions/94.html
URL	https://security.netapp.com/advisory/ntap-20170524-0001/
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03759en_us
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbns03755en_us

SSL Connection: Server Vulnerable to Heartbleed Attack — Critical

Solution Details

OpenSSL has been patched to remediate this vulnerability. Contact the vendor of the affected service, or visit the OpenSSL website, as referenced in this vulnerability, for more information on applying the patch.

The following briefly describes how to identify the vulnerable service by the port Heartbleed triggered on:

On Windows (requires Administrator privileges):
1) From a Command Prompt run: netstat -nao
2) Open the Task Manager and go to the Processes tab. Ensure the PID column is displayed, if not, go to View, Select Columns, check the box next to PID, click OK.
3) Identify the port Heartbleed triggered on in the “netstat” output and match the PID to the PID in the Task Manager.
4) The vulnerable service will be under the “Image Name” column.

-OR-

1) Download the Windows Sysinternals tool TCPView. There is a link to this tool in the External References section of this vulnerability.
2) Run it. Find the port Heartbleed triggered on and the vulnerable software will be listed under the “Process” column.

Note: On Windows, the vulnerable service will be software that was bundled with a vulnerable version of the OpenSSL library.

On Linux/Unix (requires root):
1) Run the following command: netstat -nap
2) Note the PID associated with the port that Heartbleed triggered on.
3) Run the following command, where “PID” is replaced by the PID identified in step 2: lsof | grep PID
4) Match the PID from the “netstat” output to the PID from the “lsof” output, PID is in the second column. The vulnerable service will be in the first column.

Note: On Linux/Unix it's probable that the version of OpenSSL installed on the host needs to be updated, it is also possible that a vulnerable version of OpenSSL was bundled with the identified software. Run the following to identify the version of openssl installed on the host: openssl version

Vulnerability Details

This host is vulnerable to the OpenSSL Heartbleed vulnerability. The version of the OpenSSL library on this host does not properly handle requests using the Heartbeat Extension, allowing remote attackers to harvest sensitive data from process memory. A remote unauthenticated attacker can send specially crafted Heartbeat packets to trigger a buffer over-read. OpenSSL version 1.0.1 through 1.0.1f (inclusive) is vulnerable to Heartbleed.
Impact:
An attacker can use this flaw to compromise the secret keys used to encrypt the data and communication of the affected service. Also an attacker can compromise the credentials used in the services protected by OpenSSL. With respect to the sensitivity of the data being protected, this flaw can result in a full host compromise as well as the loss of integrity of other hosts and services on the network.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160
BUGTRAQ	http://www.securityfocus.com/bid/66690
URL	http://www-01.ibm.com/support/docview.wss?uid=isg400001841
URL	http://www-01.ibm.com/support/docview.wss?uid=isg400001843
URL	http://www.splunk.com/view/SP-CAAAMB3
URL	http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
URL	http://www.vmware.com/security/advisories/VMSA-2014-0012.html
URL	http://www.openssl.org/news/vulnerabilities.html

Type	Reference
URL	https://gist.github.com/chapmajs/10473815
URL	https://support.f5.com/kb/en-us/solutions/public/15000/100/sol15159.html?sr=36517217
URL	http://heartbleed.com/
URL	http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20160512_00
URL	http://www-01.ibm.com/support/docview.wss?uid=ssg1S1004661
URL	http://www.innominate.com/data/downloads/manuals/mdm_1.5.2.1_Release_Notes.pdf
URL	https://filezilla-project.org/versions.php?type=server
URL	http://support.citrix.com/article/CTX140605
URL	http://advisories.mageia.org/MGASA-2014-0165.html
URL	https://tools.ietf.org/html/rfc6520
URL	https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-17-0008
URL	http://www.vmware.com/security/advisories/VMSA-2014-0004
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10623
URL	http://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt.aspx?ID=1
URL	http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx
URL	https://wiki.apache.org/tomcat/Security/Heartbleed
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21670858
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1084875
URL	http://www.openssl.org/news/secadv_20140407.txt

Type	Reference
URL	http://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt.aspx?ID=3
URL	http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=96db9023b881d7cd9f379b0c154650d6c108e9a3
URL	http://www.oracle.com/technetwork/topics/security/opensslheartbleedcve-2014-0160-2188454.html
URL	http://www.getchef.com/blog/2014/04/09/enterprise-chef-11-1-3-release/
URL	http://www.getchef.com/blog/2014/04/09/enterprise-chef-1-4-9-release/
URL	http://www.getchef.com/blog/2014/04/09/chef-server-11-0-12-release/
URL	http://www.kerio.com/support/kerio-control/release-history
URL	http://cogentdatahub.com/ReleaseNotes.html
URL	http://blog.fox-it.com/2014/04/08/openssl-heartbleed-bug-live-blog/
URL	http://www.f-secure.com/en/web/labs_global/fsc-2014-1
URL	http://www.getchef.com/blog/2014/04/09/chef-server-heartbleed-cve-2014-0160-releases/
URL	https://blog.torproject.org/blog/openssl-bug-cve-2014-0160
URL	https://code.google.com/p/mod-spdy/issues/detail?id=85

Threat Detected: Trojan Variant **Critical**

Solution Details

The most thorough method of cleaning up a malware infection is to wipe the hard disk of the affected machine and then perform a fresh installation of the operating system. Alternately if your antivirus vendor confirms support for cleaning of the particular variant listed in the data section, you may install an updated version of this software on the affected system and allow it to attempt to clean up the infection.

Some malicious software is able to interfere with or resist the cleanup process and in the event this happens, the best course of action is to wipe the system and perform a fresh installation.

Incident Response Checklist

1. Disconnect the computer from the network but do not turn it off. This will prevent the malicious software from propagating within your network while at the same time leaving logs and other evidence

untouched.
2. Enact your incident response program to ensure that all of the appropriate parties are aware of the incident.
3. Keep a detailed log of activities marking the date and time that any action is taken on the infected host(s).
4. Backup all files on the computer (documents, spreadsheets, etc.).
5. Determine if you will be conducting any type of forensics activity with the host.
a. If yes, engage your internal security team or external security partner so that they may conduct an investigation on the computer.
b. If no, attempt to clean in the infection with anti-virus or anti-malware software.
6. If a forensics engagement is put in place, ensure that the chain of custody of the host is maintained as to ensure that findings can be entered as evidence should the perpetrator be apprehended and court proceedings enacted.
7. To ensure that no other systems are impacted a corporate wide sweep with anti-virus and/or anti-malware should be started.
8. If any other hosts are found to be impacted use the same process as with the first infected host.
9. It should be noted that any files on the impacted system should be considered suspect and as such should be used with extreme caution.
10. If the impacted host cannot be cleaned, and there is no planned forensics analysis, the host should be wiped and reformatted. Once this done, it can be placed back into service.

Disclaimer: The steps above are general best practices and should not take the place of your formal incident response program if one is in place.

Vulnerability Details

This system appears to show evidence of having a malicious trojan horse variant installed.

Trojan horse software is any malicious computer program which misleads users of its true intent. Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an e-mail attachment disguised to be unsuspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else

Please see the data section for specifics on the evidence for this finding and links on additional information for this variant.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
URL	https://en.wikipedia.org/wiki/Trojan_horse_(computing)

Unix Server Common Password — Critical

Vulnerability Details

This host has one or more common username and password combinations that were detected.
Impact:
An attacker with knowledge of these common accounts could abuse them to log in to the host remotely and gain access to potentially sensitive information. Furthermore, it may be possible to take complete control of this host and make system changes that were not intended.

Solution Details

Please configure a strong, unique password for each account listed in the data section of this vulnerability. If possible, switch from TELNET to the Secure Shell (SSH) protocol for remotely accessing this host.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.6

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0501

Apache Chunked Encoding Buffer Overflow — High

Solution Details

Upgrade to the latest version of Apache available from vendor's website provided in the References section of this vulnerability. All versions up to and including 1.3.24 and 2.0.36 are vulnerable, for the 1.x and 2.x series, respectively. If it is not feasible to manually upgrade Apache due to the fact that the Apache web server was installed with another software package, then it is strongly advised that the vendor of the software package be contacted in order to obtain specific remediation instructions.

Vulnerability Details

This host is running Apache web server. Apache 1.3 through 1.3.24 and Apache 2.0 through 2.0.36 contain a remote buffer overflow flaw. An attacker can leverage this flaw by sending an invalid 'Chunked' encoded request to execute arbitrary commands or cause a DoS condition.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0392
BUGTRAQ	http://www.securityfocus.com/bid/5033
BUGTRAQ	http://www.securityfocus.com/bid/20005
URL	http://httpd.apache.org/info/security_bulletin_20020620.txt
URL	http://httpd.apache.org/
URL	http://httpd.apache.org/info/security_bulletin_20020617.txt

Apache httpd '2.2.32 2.4.24' Remote Segmentation Fault Vulnerability

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7668
BUGTRAQ	http://www.securityfocus.com/bid/99137
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.apple.com/HT208221
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html

Apache httpd '2.2.x before 2.2.33 and 2.4.x before 2.4.26' 'mod_mime' subcomponent Remote Read Vulnerability

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7679
BUGTRAQ	http://www.securityfocus.com/bid/99170
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03908en_us
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	https://support.apple.com/HT208221
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03821en_us
URL	https://security.netapp.com/advisory/ntap-20180601-0002/
URL	https://github.com/gottburgm/Exploits/tree/master/CVE-2017-7679
URL	https://www.nomachine.com/SU08O00185

Apache httpd '2.2.x before 2.2.33' and '2.4.x before 2.4.26' 'mod_ssl' subcomponent NULL pointer Vulnerability

High

Vulnerability Details

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3169
BUGTRAQ	http://www.securityfocus.com/bid/99134
URL	https://github.com/gottburgm/Exploits/tree/master/CVE-2017-3169
URL	https://www.nomachine.com/SU08O00185
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	https://support.apple.com/HT208221
URL	https://cwe.mitre.org/data/definitions/476.html
URL	https://security.netapp.com/advisory/ntap-20180601-0002/
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03908en_us

Apache HTTP Server 2.4.53 Security Release — High

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Affected versions of Apache HTTP Server allow a carefully crafted request body to read to a random memory area causing system crash, close inbound connections, and integer overflow causing out of bounds write. The affected versions are 2.4.52 and earlier.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22721
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22719
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23943
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22720
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server 'ap_get_basic_auth_pw' Authentication Bypass High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-3167
BUGTRAQ	http://www.securityfocus.com/bid/99135
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03908en_us

Type	Reference
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	https://www.nomachine.com/SU08O00185
URL	https://security.netapp.com/advisory/ntap-20180601-0002/
URL	https://support.apple.com/HT208221

Apache HTTP Server Internal Data Buffering Denial of Service Vulnerability — High

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

Vulnerability Details

A malicious client could perform a DoS attack by flooding a connection with requests and basically never reading responses on the TCP connection. Depending on h2 worker dimensioning, it was possible to block those with relatively few connections.
Impact:
An attacker can exploit this vulnerability to cause a denial-of-service condition, denying service to legitimate users.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9517
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server 'mod_proxy_ftp' Uninitialized Memory Usage Vulnerability — High

Vulnerability Details

Module 'mod_proxy_ftp' may use uninitialized memory when proxying to a malicious FTP server.
Impact:

An attacker could leverage this vulnerability to obtain sensitive information in the context of the affected asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1934
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server 'Module Scripts' Privilege Escalation Vulnerability

High

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

Vulnerability Details

In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
Impact:
Attackers can exploit this issue to elevate their privilege level and execute arbitrary code in the context of the affected asset, possibly leading to a complete compromise of the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0211

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/107666
URL	https://httpd.apache.org/download.cgi
URL	https://www.synology.com/security/advisory/Synology_SA_19_14
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	http://packetstormsecurity.com/files/152386/Apache-2.4.38-Root-Privilege-Escalation.html
URL	http://packetstormsecurity.com/files/152415/Slackware-Security-Advisory-httpd-Updates.html
URL	http://packetstormsecurity.com/files/152441/CARPE-DIEM-Apache-2.4.x-Local-Privilege-Escalation.html
URL	http://www.apache.org/dist/httpd/CHANGES_2.4.39
URL	https://support.f5.com/csp/article/K32957101
URL	https://security.netapp.com/advisory/ntap-20190423-0001/

Apache HTTP Server Security Update 2.4.48 High

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

Vulnerability Details

Apache HTTP Server's mod_proxy_wstunnel, mod_proxy_http, and mod_auth_digest have vulnerabilities that can range from Denial-of-Service to Stack/heap overflows.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31618
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-17567

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-35452
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30641
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26691
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26690
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13950
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-13938
URL	https://httpd.apache.org/download.cgi
URL	http://httpd.apache.org/security/vulnerabilities_24.html
URL	https://httpd.apache.org/security/vulnerabilities_24.html

Apache HTTP Server Security Update 2.4.51 High

Solution Details

Please upgrade to the latest version.

Vulnerability Details

A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain Socket endpoint (Server Side Request Forgery). Also, A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts).

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-44790
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-44224

Type	Reference
URL	https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BFSWOH4X77CV7AH7C4RMHUBDWKQDL4YH/
URL	https://httpd.apache.org/security/vulnerabilities_24.html

Apache Tomcat "Ghostcat" AJP Local File Inclusion and RCE — High

Solution Details

Apache Tomcat developers have released Tomcat versions 7.0.100, 8.5.51, and 9.0.31, which include changes to the default server.xml configuration file which disable the AJP connector by default. It should be noted that reenabling the connector without ensuring other configuration changes are made may result in the asset becoming vulnerable again.

If the AJP connector is not required, ensure it is disabled.

If the AJP connector is required, and is not run on a trusted network, ensure that the secretRequired directive is set in its definition in the server.xml file.

Vulnerability Details

The Apache Tomcat AJP connector may permit remote, unauthenticated attackers to obtain arbitrary files from the web directory of an affected Tomcat instance. Additionally, JSP files will be executed, which if combined with the ability to upload a file to the server, may result in remote code execution.

The AJP connector is enabled by default and listens on all interfaces on Apache Tomcat versions 7.0.0-7.0.99, 8.5.0-8.5.50, and 9.0.0-9.0.30.
Impact:
A remote, unauthenticated attacker may be able to leverage this vulnerability to retrieve arbitrary files from the affected Tomcat instance's web directory, including configuration files.

If the attacker also possesses the ability to upload files to the affected Tomcat instance, and the files are stored within the web directory, it may be possible for a remote, unauthenticated attacker to execute arbitrary code with the privileges of the affected Tomcat instance.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1938

Apache Win32 Directory Traversal High

Vulnerability Details

This host is running Apache. Apache 2.0 - 2.0.39 on Windows, OS2, and Netware contains a directory traversal flaw. Remote attackers can leverage a URI containing "..\" or "../" character sequences to access host files and execute arbitrary commands.

False Positive Notes

This item may be a false positive under certain conditions or if a backported solution has been applied. Please validate and document remediation efforts through Active View.

Solution Details

Please update to the most recent version of Apache from the vendor linked in the References List of the vulnerability details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-0661
BUGTRAQ	http://www.securityfocus.com/bid/5434
URL	http://httpd.apache.org/info/security_bulletin_20020908a.txt
URL	http://httpd.apache.org/

Easily Guessable MySQL Credentials High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please reconfigure this host to use a unique username and a secure password for each authorized user. Passwords should be of sufficient length and complexity as specified in the organization's password policy.

Vulnerability Details

This host is running a MySQL instance configured to use an easily guessable username and password combination. An attacker can leverage this configuration to gain access to this host.

Impact:
An attacker can leverage this vulnerability to harvest sensitive data from the database. An attacker can also potentially execute arbitrary commands, which would yield a full compromise of the host.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
URL	http://dev.mysql.com/doc/refman/5.0/en/set-password.html

Easily Guessable Telnet Credentials — High

Solution Details

Ensure that all accounts are using complex and hard to guess passwords.

Vulnerability Details

This host is running a telnet server that contains user accounts with easily guessable credentials.
Impact:
An attacker can leverage this flaw to remotely manage this host and possibly gain sensitive information. The scope of a compromise by an attacker depends heavily on the user account permissions. Limited access user accounts will have less ability to gain access to restricted files and should have less control over the remote host. If the user account is an administrative account, an attacker could take complete control of this host and its content.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
There are no references for this vulnerability.	

Fileinfo 'file_check_mem' Arbitrary Code Execution — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8865
BUGTRAQ	http://www.securityfocus.com/bid/85802
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	https://bugs.php.net/bug.php?id=71527
URL	https://github.com/file/file/commit/6713ca45e7757297381f4b4cdb9cf5e624a9ad36
URL	http://www.php.net/ChangeLog-7.php
URL	https://support.apple.com/HT206567
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://git.php.net/?p=php-src.git;a=commit;h=fe13566c93f118a15a96320a546c7878fd0cfc5e

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 100.0.1185.29 — High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 100.0.1185.29. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the

100.0.1185.29 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.1

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26891
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1125
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1131
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1135
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1136
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1137
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1127
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1138
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1128
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1133
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1134
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1129
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1139
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1146
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1143
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1130
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24523
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24475

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26912
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26908
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26900
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26894
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26909
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26895
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26891
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24523
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24475
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26912
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26908
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26900
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26894
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26909
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26895

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 100.0.1185.36 — High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser

window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 100.0.1185.36. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 100.0.1185.36 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.1

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1232

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 100.0.1185.44

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 100.0.1185.44. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 100.0.1185.44 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.1

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1364
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29144

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 101.0.1210.32

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 101.0.1210.32. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 101.0.1210.32 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.1

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1500
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29146
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29147
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1479
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1491
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1484

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1483
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1487
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1477
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1498
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1490
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1495
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1482
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1499
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1492
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1485
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1488
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1501
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1486
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1497
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1478
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1481
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1493
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1494

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 101.0.1210.47

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 101.0.1210.47. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 101.0.1210.47 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.1

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1640
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1638
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1637
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1635
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1634
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1636
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1639

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 102.0.1245.30

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 102.0.1245.30. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the

102.0.1245.30 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.3

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1871
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1876
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1863
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1856
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1869
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1868
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1862
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1855
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1853
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1865
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1872
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1854
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1864
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30128
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30127
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26905
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1867
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1874
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1857

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1873
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1859
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1870
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1875

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 102.0.1245.39 — High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 102.0.1245.39. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 102.0.1245.39 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.1

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22021

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 102.0.1245.41 — High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 102.0.1245.41. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 102.0.1245.41 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.1

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2008
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2007
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2011
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2010

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 103.0.1264.37

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 103.0.1264.37. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the

103.0.1264.37 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.3

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2156
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33638
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30192
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33639
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2165
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2160
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2162
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2157
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2158
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2161
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2163
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2164

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 103.0.1264.44

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 103.0.1264.44. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 103.0.1264.44 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.3

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33680
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33680

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 103.0.1264.49 — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 103.0.1264.49. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 103.0.1264.49 update to correct these issues.

Please see the CVE's linked in the references list for more information.

CVSS Base Score: 7.1

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2294

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 92.0.902.78

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 92.0.902.78. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 92.0.902.78 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30602
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30604
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30599
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30603
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30598
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30601

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.38

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 93.0.961.38. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 93.0.961.38 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.1

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38641
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26439
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36930
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26436
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38642

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.44

High

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 93.0.961.44. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 93.0.961.44

update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38669

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.47 — High

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 93.0.961.47. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 93.0.961.47 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30632

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 93.0.961.52 — High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 93.0.961.52. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 93.0.961.52 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.6

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30633
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30628
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30626
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30627
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30629
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30625
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30630

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 94.0.992.31

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 94.0.992.31. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 94.0.992.31 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37961
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37956
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37959
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37973
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37968
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37964
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37971
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37966
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37957
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37970

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37969
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37958
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37962
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37963
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37967
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37965
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37972

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 94.0.992.38

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 94.0.992.38. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 94.0.992.38 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37975
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37976

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37974
URL	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_30.html

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 94.0.992.47

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 94.0.992.47. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 94.0.992.47 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37977
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37978
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37979
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37980

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 95.0.1020.30

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 95.0.1020.30. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 95.0.1020.30 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9

CVSS Vector: AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41330
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41342
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41361
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41335
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41357
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41347
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40478
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40449
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38662
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40463
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41338
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41331

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40455
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40466
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41339
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40477
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40467
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40456
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36953
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40488
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41345
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40469
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40461
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41334
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40443
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41343
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40450
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40465
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40462
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36970
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40468
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40489
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41332
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40464
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40470
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26441

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38672
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41336
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40460
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41346
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41340
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38663
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41337
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40476
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40475
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26442
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40454
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41336
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40477
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41339
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40466
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38672
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26441
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40455
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40463
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40470

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41331
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41338
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38662
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40449
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40478
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40464
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41347
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41332
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40489
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41357
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40468
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41335
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41361
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41342
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40456
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41346

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36953
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40488
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41345
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41330
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40469
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40461
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41340
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41334
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38663
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40443
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41343
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40450
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41337
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40476
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40475
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26442

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40465
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40462
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36970
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40454
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40467
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40460

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 95.0.1020.40 High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 95.0.1020.40. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 95.0.1020.40 update to correct these issues.

Please see the CVE's linked in the references list for more information.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38000
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38003
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38001
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37997
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38002
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37998
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37999

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 96.0.1054.29 — High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 96.0.1054.29. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 96.0.1054.29 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38018
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38015

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38013
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38016
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38021
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38006
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38011
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38010
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38009
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38008
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38020
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38007
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38005
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38022
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38014
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38012
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43221
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42308
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38019
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38017

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 96.0.1054.57 — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 96.0.1054.57. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 96.0.1054.57 update to correct these issues.

Please see the CVE's linked in the references list for more information.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4099
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4100
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4102
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4098
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4101

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 97.0.1072.55

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 97.0.1072.55. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 97.0.1072.55 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21954
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21970
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21929
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21930
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21931

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 97.0.1072.69

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 97.0.1072.69. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 97.0.1072.69 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23258

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 98.0.1108.43

High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 98.0.1108.43. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 98.0.1108.43 update to correct these issues.

Please see the CVE's linked in the references list for more information.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23261
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23262
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23263
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23262
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23263
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23261

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 98.0.1108.50

High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 98.0.1108.50. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 98.0.1108.50 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.1

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23264

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 98.0.1108.55 — High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 98.0.1108.55. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 98.0.1108.55 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0610
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0607
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0603
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0608
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0609
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0606
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0604
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0605

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 99.0.1150.30 — High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 99.0.1150.30. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 99.0.1150.30 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0797
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0808
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0798
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0796
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0804
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0800
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0790
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0809
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0799
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0792
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0802
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0807
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0806
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0789
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0793
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0803
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0795
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0805
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0801
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0791
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0794

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 99.0.1150.46

High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 99.0.1150.46. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 99.0.1150.46 update to correct these issues.

Please see the CVE's linked in the references list for more information.

CVSS Base Score: 7.1

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26899
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0979
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0975
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0971
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0973
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0972
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0977
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0974
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0980
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0976
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0978

Microsoft Edge (Chromium): Multiple Vulnerabilities in Versions Less Than 99.0.1150.55 — High

Solution Details

To manually update Microsoft Edge (Chromium) to the latest version do the following:

a) Click the menu button (looks like three horizontal dots) on the right-hand corner of the Edge browser window.
b) Scroll down to 'Help & Feedback'.
c) Click on 'About Microsoft Edge'.

Vulnerability Details

Microsoft Edge (Chromium) is affected by multiple vulnerabilities in versions less than 99.0.1150.55. These flaws include both denial of service, and memory corruption flaws that could allow a remote attacker to run arbitrary code within the context of the browser. Microsoft has released the 99.0.1150.55 update to correct these issues.

Please see the CVE's linked in the references list for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.1

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1096

Microsoft Windows 7 End of Life — High

Solution Details

Upgrade to a supported version of Microsoft Windows.

Vulnerability Details

This asset is running a version of Windows 7 that has reached end of life status. As such, newly discovered vulnerabilities will no longer be patched by the vendor.
Impact:
Even though vulnerabilities in this version of Windows 7 may exist, Microsoft will not patch them. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this asset or its data.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

Microsoft Windows Server 2008 End of Life — High

Vulnerability Details

This asset is running a version of Windows Server 2008 that has reached end of life status. As such, newly discovered vulnerabilities will no longer be patched by the vendor.
Impact:
Even though vulnerabilities in this version of Windows Server 2008 may exist, Microsoft will not patch them. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this asset or its data.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to a supported version of Microsoft Windows.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://www.microsoft.com/en-us/cloud-platform/windows-server-2008

Microsoft Windows Server 2008 R2 End of Life — High

Solution Details

Upgrade to a supported version of Microsoft Windows.

Vulnerability Details

This asset is running a version of Windows Server 2008 R2 that has reached end of life status. As such, newly discovered vulnerabilities will no longer be patched by the vendor.
Impact:
Even though vulnerabilities in this version of Windows Server 2008 R2 may exist, Microsoft will not patch them. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this asset or its data.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://www.microsoft.com/en-us/cloud-platform/windows-server-2008

Microsoft Windows XP End of Life — High

Solution Details

If this host is required for production, please upgrade the operating system and ensure it is fully patched.

Vulnerability Details

This host is running a version of Microsoft Windows which is no longer supported by Microsoft. Vulnerabilities associated with this version of Windows cannot be guaranteed to be patched by Microsoft. This outdated operating system could be leveraged to compromise the host or to assist in other attacks.

Impact:
Unsupported versions of Microsoft Windows will no longer get updates from Microsoft. As such, this OS can be susceptible to vulnerabilities identified in other versions of Windows without any chance of being remediated.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	http://windows.microsoft.com/en-us/windows/end-support-help

MS12-020 Remote Desktop Protocol Use-After-Free Vulnerability (Network Check) — High

Solution Details

Microsoft has released patch MS12-020 to address the issue. MS12-020 covers two separate issues related to the Remote Desktop Protocol (RDP) service. This vulnerability description pertains to the issue covered by KB2621440.

Due to the fact that the affected code resides in a kernel driver of the Microsoft Windows operating system, application of the patch requires a reboot of the affected system.

Note: On June 12, 2012, KB2621440 was replaced by KB2685939 (MS12-036). Microsoft Automatic Updates and Microsoft Baseline Security Analyzer will show that the vulnerable system is missing security update MS12-036 instead of MS12-020.
Workarounds:
Microsoft has suggested that Network Level Authentication is a sufficient workaround for mitigating the flaw described in CVE-2012-0002. This does not prevent an attacker from exploiting the issue, but provides a higher barrier to entry in that the attacker must provide some level of authentication prior to exploiting the vulnerability. The Network Level Authentication feature of the Remote Desktop Services implementation is available on Microsoft Windows Vista and later.

The secondary issue, which is described by CVE-2012-0152, will not be mitigated by enabling Network Level Authentication.

If the Remote Desktop Services is not necessary, disabling the service is a valid workaround.

Vulnerability Details

The Remote Desktop Services installation on the remote host contains a use-after-free vulnerability which can allow a remote unauthenticated attacker to execute arbitrary code under the context of the kernel driver. Failed exploit attempts will cause a denial of service condition on the affected host.

The use-after-free vulnerability occurs when the 'maxChannelIds' field of the T.125 ConnectMCSPDU packet has a value which is exceeded by the number of channels that are requested in the subsequent GCC Conference Create packet. Requesting a number of channels which exceeds the value in the maxChannelIds field will cause the processing code to abort the connection and will trigger a code sequence which attempts to execute data based on a pointer which has previously been freed.

While exploiting this issue to execute controlled code is difficult, triggering the denial of service condition is trivial.
Impact:
An attacker who successfully exploits the use-after-free vulnerability will gain arbitrary code execution on the remote host under the context of the kernel driver. Failed attempts will result in a denial of service condition which will likely be exhibited by a blue screen.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0002
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0152

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/52354
MSB	http://technet.microsoft.com/security/bulletin/MS12-020
URL	https://cwe.mitre.org/data/definitions/94.html
URL	http://aluigi.altervista.org/adv/termdd_1-adv.txt
URL	http://www.zerodayinitiative.com/advisories/ZDI-12-044/
URL	http://isc.sans.edu/diary.html?storyid=12808
URL	http://blogs.quickheal.com/remote-desktop-protocol-vulnerability-cve-2012-0002-not-dead-yet/
URL	https://cwe.mitre.org/data/definitions/20.html

MS13-098: Vulnerability in Windows Could Allow Remote Code Execution - Registry Entry Not Set

High

Solution Details

Confirm that the following registry keys are set to 1 (one):
For 32-bit versions of Microsoft Windows:
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config
EnableCertPaddingCheck = 1 (DWORD)

For 64-bit versions of Microsoft Windows:
HKEY_LOCAL_MACHINE\Software\Microsoft\Cryptography\Wintrust\Config
EnableCertPaddingCheck = 1 (DWORD)

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Cryptography\Wintrust\Config
EnableCertPaddingCheck = 1 (DWORD)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This security update resolves a privately reported vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if user or application runs or installs a specially crafted, signed portable executable (PE) file on an affected system.

The Microsoft patch for this vulnerability has been installed, but registry values have not been set that are required to fully remediate the vulnerability.
Impact:

An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

CVSS Base Score: 7.6

CVSS Vector: AV:N/AC:H/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-3900
URL	http://blogs.technet.com/b/srd/archive/2013/12/10/ms13-098-update-to-enhance-the-security-of-authenticode.aspx
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2013-3900

MS14-068: Vulnerability in Kerberos Could Allow Elevation of Privilege

High

Solution Details

Microsoft has released a fix for this flaw in their 'MS14-068' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

This security update resolves a privately reported vulnerability in Microsoft Windows Kerberos KDC that could allow an attacker to elevate unprivileged domain user account privileges to those of the domain administrator account. An attacker could use these elevated privileges to compromise any computer in the domain, including domain controllers. An attacker must have valid domain credentials to exploit this vulnerability. The affected component is available remotely to users who have standard user accounts with domain credentials; this is not the case for users with local account credentials only. When this security bulletin was issued, Microsoft was aware of limited, targeted attacks that attempt to exploit this vulnerability.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS14-068'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9

CVSS Vector: AV:N/AC:L/Au:S/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6324
BUGTRAQ	http://www.securityfocus.com/bid/70958
MSB	http://technet.microsoft.com/security/bulletin/MS14-068
URL	http://blogs.technet.com/b/srd/archive/2014/11/18/additional-information-about-cve-2014-6324.aspx

MS15-009: Security Update for Internet Explorer — High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-009'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-009' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0050
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0054
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0027
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0031
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0030
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0051
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0055
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0053
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0052
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0041
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0042
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0043
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0022
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0044
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0040

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0045
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0039
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0023
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0071
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0070
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0046
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0037
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0069
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0021
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0068
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0017
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8967
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0038
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0025
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0048
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0018
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0019
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0036
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0020
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0028
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0026
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0067
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0035
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0049

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0066
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0029
BUGTRAQ	http://www.securityfocus.com/bid/72446
BUGTRAQ	http://www.securityfocus.com/bid/72478
BUGTRAQ	http://www.securityfocus.com/bid/72441
BUGTRAQ	http://www.securityfocus.com/bid/72444
BUGTRAQ	http://www.securityfocus.com/bid/72442
BUGTRAQ	http://www.securityfocus.com/bid/72421
BUGTRAQ	http://www.securityfocus.com/bid/72479
BUGTRAQ	http://www.securityfocus.com/bid/72443
BUGTRAQ	http://www.securityfocus.com/bid/72418
BUGTRAQ	http://www.securityfocus.com/bid/72420
BUGTRAQ	http://www.securityfocus.com/bid/72410
BUGTRAQ	http://www.securityfocus.com/bid/72411
BUGTRAQ	http://www.securityfocus.com/bid/72412
BUGTRAQ	http://www.securityfocus.com/bid/72413
BUGTRAQ	http://www.securityfocus.com/bid/72436
BUGTRAQ	http://www.securityfocus.com/bid/72414
BUGTRAQ	http://www.securityfocus.com/bid/72409
BUGTRAQ	http://www.securityfocus.com/bid/72437
BUGTRAQ	http://www.securityfocus.com/bid/72404
BUGTRAQ	http://www.securityfocus.com/bid/72415
BUGTRAQ	http://www.securityfocus.com/bid/72455
BUGTRAQ	http://www.securityfocus.com/bid/72480

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/72454
BUGTRAQ	http://www.securityfocus.com/bid/72448
BUGTRAQ	http://www.securityfocus.com/bid/72402
BUGTRAQ	http://www.securityfocus.com/bid/72438
BUGTRAQ	http://www.securityfocus.com/bid/72419
BUGTRAQ	http://www.securityfocus.com/bid/72424
BUGTRAQ	http://www.securityfocus.com/bid/72416
BUGTRAQ	http://www.securityfocus.com/bid/72426
BUGTRAQ	http://www.securityfocus.com/bid/71483
BUGTRAQ	http://www.securityfocus.com/bid/72439
BUGTRAQ	http://www.securityfocus.com/bid/72403
BUGTRAQ	http://www.securityfocus.com/bid/72425
BUGTRAQ	http://www.securityfocus.com/bid/72453
BUGTRAQ	http://www.securityfocus.com/bid/72440
BUGTRAQ	http://www.securityfocus.com/bid/72423
BUGTRAQ	http://www.securityfocus.com/bid/72447
BUGTRAQ	http://www.securityfocus.com/bid/72422
BUGTRAQ	http://www.securityfocus.com/bid/72417
BUGTRAQ	http://www.securityfocus.com/bid/72445
MSB	http://technet.microsoft.com/security/bulletin/MS15-009
URL	http://blog.skylined.nl/20161114001.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://blog.skylined.nl/20161122001.html
URL	http://zerodayinitiative.com/advisories/ZDI-14-403/

Type	Reference
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-009

MS15-010: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution

High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-010'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-010' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0059
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0058
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0057
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0010
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0003
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0060
BUGTRAQ	http://www.securityfocus.com/bid/72468
BUGTRAQ	http://www.securityfocus.com/bid/72466
BUGTRAQ	http://www.securityfocus.com/bid/72461
BUGTRAQ	http://www.securityfocus.com/bid/72457
BUGTRAQ	http://www.securityfocus.com/bid/72472
BUGTRAQ	http://www.securityfocus.com/bid/72470
MSB	http://technet.microsoft.com/security/bulletin/MS15-010
URL	https://cwe.mitre.org/data/definitions/476.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-010
URL	https://cwe.mitre.org/data/definitions/310.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/415.html
URL	http://code.google.com/p/google-security-research/issues/detail?id=128
URL	https://cwe.mitre.org/data/definitions/20.html

MS15-018: Cumulative Security Update for Internet Explorer High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-018'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-018' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1626
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1634
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0100
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0099
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0056
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1622

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1623
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1624
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1625
BUGTRAQ	http://www.securityfocus.com/bid/72923
BUGTRAQ	http://www.securityfocus.com/bid/72930
BUGTRAQ	http://www.securityfocus.com/bid/72931
BUGTRAQ	http://www.securityfocus.com/bid/72925
BUGTRAQ	http://www.securityfocus.com/bid/72924
BUGTRAQ	http://www.securityfocus.com/bid/72926
BUGTRAQ	http://www.securityfocus.com/bid/72927
BUGTRAQ	http://www.securityfocus.com/bid/72928
BUGTRAQ	http://www.securityfocus.com/bid/72929
MSB	http://technet.microsoft.com/security/bulletin/MS15-018
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-018
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/399.html

MS15-021: Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution

High

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-021' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-021'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0088
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0087
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0074
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0089
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0090
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0091
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0092
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0093
BUGTRAQ	http://www.securityfocus.com/bid/72892
BUGTRAQ	http://www.securityfocus.com/bid/72898
BUGTRAQ	http://www.securityfocus.com/bid/72896
BUGTRAQ	http://www.securityfocus.com/bid/72904

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/72905
BUGTRAQ	http://www.securityfocus.com/bid/72906
BUGTRAQ	http://www.securityfocus.com/bid/72907
BUGTRAQ	http://www.securityfocus.com/bid/72893
MSB	http://technet.microsoft.com/security/bulletin/MS15-021
URL	https://cwe.mitre.org/data/definitions/94.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html

MS15-032: Cumulative Security Update for Internet Explorer High

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-032' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-032'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1660
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1659
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1657
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1652
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1661
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1662
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1665
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1666
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1667
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1668
BUGTRAQ	http://www.securityfocus.com/bid/73994
BUGTRAQ	http://www.securityfocus.com/bid/74006
BUGTRAQ	http://www.securityfocus.com/bid/74000
BUGTRAQ	http://www.securityfocus.com/bid/74004
BUGTRAQ	http://www.securityfocus.com/bid/73990
MSB	http://technet.microsoft.com/security/bulletin/MS15-032
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-032
URL	https://cwe.mitre.org/data/definitions/399.html

MS15-034: Microsoft IIS HTTP.sys Remote Code Execution (Network Check) — High

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-034' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch requires a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-034'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1635
BUGTRAQ	http://www.securityfocus.com/bid/74013
MSB	http://technet.microsoft.com/security/bulletin/MS15-034
URL	http://packetstormsecurity.com/files/131463/Microsoft-Windows-HTTP.sys-Proof-Of-Concept.html
URL	https://technet.microsoft.com/en-us/library/security/ms15-034.aspx
URL	https://cwe.mitre.org/data/definitions/94.html

MS15-043: Cumulative Security Update for Internet Explorer High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-043' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to knock it offline, denying service to legitimate users.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-043'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1705
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1689
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1708
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1711

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1710
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1688
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1717
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1709
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1685
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1714
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1713
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1691
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1686
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1706
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1684
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1694
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1703
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1704
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1718
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1712
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1658
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1692
BUGTRAQ	http://www.securityfocus.com/bid/74509
BUGTRAQ	http://www.securityfocus.com/bid/74510
BUGTRAQ	http://www.securityfocus.com/bid/74514
BUGTRAQ	http://www.securityfocus.com/bid/74513
BUGTRAQ	http://www.securityfocus.com/bid/74519

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/74504
BUGTRAQ	http://www.securityfocus.com/bid/74511
BUGTRAQ	http://www.securityfocus.com/bid/74530
BUGTRAQ	http://www.securityfocus.com/bid/74516
BUGTRAQ	http://www.securityfocus.com/bid/74505
BUGTRAQ	http://www.securityfocus.com/bid/74506
BUGTRAQ	http://www.securityfocus.com/bid/74522
BUGTRAQ	http://www.securityfocus.com/bid/74512
BUGTRAQ	http://www.securityfocus.com/bid/74508
BUGTRAQ	http://www.securityfocus.com/bid/74520
BUGTRAQ	http://www.securityfocus.com/bid/74521
BUGTRAQ	http://www.securityfocus.com/bid/74607
BUGTRAQ	http://www.securityfocus.com/bid/74606
BUGTRAQ	http://www.securityfocus.com/bid/74518
BUGTRAQ	http://www.securityfocus.com/bid/74507
BUGTRAQ	http://www.securityfocus.com/bid/74517
BUGTRAQ	http://www.securityfocus.com/bid/74515
MSB	http://technet.microsoft.com/security/bulletin/MS15-053
MSB	http://technet.microsoft.com/security/bulletin/MS15-043
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-043
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html

MS15-044: Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution

High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-044' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-044'.

Affected Products Are:
- Microsoft Live Meeting 2007 Console
- Microsoft Lync 2010 (32-bit)
- Microsoft Lync 2010 (64-bit)
- Microsoft Lync 2010 Attendee (admin level install)
- Microsoft Lync 2010 Attendee (user level install)
- Microsoft Lync 2013
- Microsoft Lync Basic 2013
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Silverlight 5 Developer Runtime when installed on Apple Mac OS (Intel-based)
- Microsoft Silverlight 5 Developer Runtime when installed on Microsoft Windows (32-bit)
- Microsoft Silverlight 5 Developer Runtime when installed on Microsoft Windows (x64-based)
- Microsoft Silverlight 5 when installed on Apple Mac OS (Intel-based)
- Microsoft Silverlight 5 when installed on Microsoft Windows (32-bit)
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1671
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1670
BUGTRAQ	http://www.securityfocus.com/bid/74490
BUGTRAQ	http://www.securityfocus.com/bid/74485
MSB	http://technet.microsoft.com/security/bulletin/MS15-044
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-044

MS15-056: Cumulative Security Update for Internet Explorer — High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-056'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-056' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1743
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1765
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1687
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1742
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1755
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1766
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1739
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1748
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1741
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1750
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1747
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1730
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1754
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1751
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1731
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1732
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1735
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1736
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1737

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1740
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1745
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1753
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1752
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1744
BUGTRAQ	http://www.securityfocus.com/bid/74996
BUGTRAQ	http://www.securityfocus.com/bid/74994
BUGTRAQ	http://www.securityfocus.com/bid/74991
BUGTRAQ	http://www.securityfocus.com/bid/74983
BUGTRAQ	http://www.securityfocus.com/bid/74982
BUGTRAQ	http://www.securityfocus.com/bid/74995
BUGTRAQ	http://www.securityfocus.com/bid/74979
BUGTRAQ	http://www.securityfocus.com/bid/74997
BUGTRAQ	http://www.securityfocus.com/bid/74993
BUGTRAQ	http://www.securityfocus.com/bid/74986
BUGTRAQ	http://www.securityfocus.com/bid/74992
BUGTRAQ	http://www.securityfocus.com/bid/74981
BUGTRAQ	http://www.securityfocus.com/bid/74972
BUGTRAQ	http://www.securityfocus.com/bid/74990
BUGTRAQ	http://www.securityfocus.com/bid/74978
BUGTRAQ	http://www.securityfocus.com/bid/74985
BUGTRAQ	http://www.securityfocus.com/bid/74989
BUGTRAQ	http://www.securityfocus.com/bid/74987
BUGTRAQ	http://www.securityfocus.com/bid/74984

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/74988
MSB	http://technet.microsoft.com/security/bulletin/MS15-056
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-254
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-056
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-249
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-250
URL	https://cwe.mitre.org/data/definitions/19.html
URL	http://blog.skylined.nl/20161206001.html
URL	http://packetstormsecurity.com/files/140050/Microsoft-Internet-Explorer-9-jscript9-JavaScriptStackWalker-Memory-Corruption.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-253
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-252
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-251
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-377

MS15-065: Security Update for Internet Explorer — High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-065'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition

- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-065' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2412
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2413
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2419
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2421
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2422
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2425
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2414
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1729
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1733
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1738
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1767
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2383

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2384
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2385
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2388
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2389
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2390
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2391
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2397
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2398
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2401
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2402
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2403
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2404
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2406
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2408
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2410
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2411
BUGTRAQ	http://www.securityfocus.com/bid/75677
BUGTRAQ	http://www.securityfocus.com/bid/75687
MSB	http://technet.microsoft.com/security/bulletin/MS15-065
URL	https://cwe.mitre.org/data/definitions/79.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-065
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-568
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-458

MS15-078: Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution	High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-078'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-078' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2426

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/75951
MSB	http://technet.microsoft.com/security/bulletin/MS15-078
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-078
URL	http://blog.trendmicro.com/trendlabs-security-intelligence/a-look-at-the-open-type-font-manager-vulnerability-from-the-hacking-team-leak/

MS15-079: Cumulative Security Update for Internet Explorer

High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-079'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-079' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2443
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2452
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2451
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2450
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2448
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2447
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2446
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2445
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2423
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2441
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2444
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2449
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2442
BUGTRAQ	http://www.securityfocus.com/bid/76195
BUGTRAQ	http://www.securityfocus.com/bid/76188
BUGTRAQ	http://www.securityfocus.com/bid/76189
BUGTRAQ	http://www.securityfocus.com/bid/76190
BUGTRAQ	http://www.securityfocus.com/bid/76191
BUGTRAQ	http://www.securityfocus.com/bid/76194
MSB	http://technet.microsoft.com/security/bulletin/MS15-091
MSB	http://technet.microsoft.com/security/bulletin/MS15-088
MSB	http://technet.microsoft.com/security/bulletin/MS15-081
MSB	http://technet.microsoft.com/security/bulletin/MS15-079

Type	Reference
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-382
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-079
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html

MS15-080: Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution

High

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-080' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-080'.

Affected Products Are:
- Microsoft Live Meeting 2007 Console
- Microsoft Lync 2010 (32-bit)
- Microsoft Lync 2010 (64-bit)
- Microsoft Lync 2010 Attendee (admin level install)
- Microsoft Lync 2010 Attendee (user level install)
- Microsoft Lync 2013
- Microsoft Lync Basic 2013
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Silverlight 5 Developer Runtime when installed on Apple Mac OS (Intel-based)
- Microsoft Silverlight 5 Developer Runtime when installed on Microsoft Windows (32-bit)
- Microsoft Silverlight 5 Developer Runtime when installed on Microsoft Windows (x64-based)
- Microsoft Silverlight 5 when installed on Apple Mac OS (Intel-based)
- Microsoft Silverlight 5 when installed on Microsoft Windows (32-bit)
- Windows 10
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT

- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2433
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2453
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2432
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2431
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2465
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2464
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2463
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2462
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2461
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2460
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2459
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2458
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2456
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2454
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2455
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2435

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/76238
BUGTRAQ	http://www.securityfocus.com/bid/76240
BUGTRAQ	http://www.securityfocus.com/bid/76239
BUGTRAQ	http://www.securityfocus.com/bid/76215
BUGTRAQ	http://www.securityfocus.com/bid/76209
BUGTRAQ	http://www.securityfocus.com/bid/76241
BUGTRAQ	http://www.securityfocus.com/bid/76216
BUGTRAQ	http://www.securityfocus.com/bid/76213
MSB	http://technet.microsoft.com/security/bulletin/MS15-080
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-387
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-080
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/19.html

MS15-093: Security Update for Internet Explorer — High

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-093' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-093'.

Affected Products Are:
- Windows 10

- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2502
BUGTRAQ	http://www.securityfocus.com/bid/76403
MSB	http://technet.microsoft.com/security/bulletin/MS15-093
URL	http://www.securityweek.com/microsoft-issues-emergency-patch-critical-ie-flaw-exploited-wild
URL	https://cwe.mitre.org/data/definitions/119.html

MS15-106: Cumulative Security Update for Internet Explorer High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-106'.

Affected Products Are:
- Windows 10
- Windows 7

- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-106' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6045
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6049
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6053
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6056
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6048
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6047
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6046
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6044
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6042
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6059
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6055
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6052
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6050

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6051
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2482
BUGTRAQ	http://www.securityfocus.com/bid/76991
BUGTRAQ	http://www.securityfocus.com/bid/77010
MSB	http://technet.microsoft.com/security/bulletin/MS15-108
MSB	http://technet.microsoft.com/security/bulletin/MS15-106
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-545
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-518
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-522
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-523
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-523/
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-520
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-537
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-521
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-515
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-106

MS15-124: Cumulative Security Update for Internet Explorer — High

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-124' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS15-124'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6150
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6149
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6147
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6146
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6144
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6143
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6141
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6138
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6135

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6136
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6139
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6142
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6148
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6151
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6153
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6154
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6155
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6158
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6159
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6161
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6083
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6134
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6140
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6156
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6164
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6162
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6160
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6157
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6152
MSB	http://technet.microsoft.com/security/bulletin/MS15-124
MSB	http://technet.microsoft.com/security/bulletin/MS15-126
MSB	http://technet.microsoft.com/security/bulletin/MS15-125
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-589

Type	Reference
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-584
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-585
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-600
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-586
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-591
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-592
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-593
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-594
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-595
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-597
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-598
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-587
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-588
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-599
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-124
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-645
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-647
URL	https://cwe.mitre.org/data/definitions/79.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-582
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-590

MS16-001: Cumulative Security Update for Internet Explorer High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-001'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-001' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0005
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0002
MSB	http://technet.microsoft.com/security/bulletin/MS16-001
MSB	http://technet.microsoft.com/security/bulletin/MS16-003
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-001

Type	Reference
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/20.html

MS16-009: Cumulative Security Update for Internet Explorer

High

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-009' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-009'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0069
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0077

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0072
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0071
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0041
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0062
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0061
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0063
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0064
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0067
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0068
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0060
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0059
BUGTRAQ	http://www.securityfocus.com/bid/82665
MSB	http://technet.microsoft.com/security/bulletin/MS16-009
MSB	http://technet.microsoft.com/security/bulletin/MS16-014
MSB	http://technet.microsoft.com/security/bulletin/MS16-011
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-157
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-009
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-158
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-162
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-165
URL	https://cwe.mitre.org/data/definitions/19.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-166

Type	Reference
URL	http://blog.skylined.nl/20161128001.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-159
URL	https://www.securify.nl/advisory/SFY20150905/nps_datastore_server_dll_side_loading_vulnerability.html

MS16-012: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution

High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-012'.

Affected Products Are:
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-012' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0046
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0058
MSB	http://technet.microsoft.com/security/bulletin/MS16-012

Type	Reference
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-012
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-156

MS16-023: Cumulative Security Update for Internet Explorer — High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-023'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-023' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0108
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0103
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0104
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0105
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0106
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0109
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0102
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0111
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0114
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0113
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0112
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0107
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0110
BUGTRAQ	http://www.securityfocus.com/bid/84010
BUGTRAQ	http://www.securityfocus.com/bid/84013
BUGTRAQ	http://www.securityfocus.com/bid/84019
BUGTRAQ	http://www.securityfocus.com/bid/84015
BUGTRAQ	http://www.securityfocus.com/bid/84018
BUGTRAQ	http://www.securityfocus.com/bid/84020
BUGTRAQ	http://www.securityfocus.com/bid/84021
BUGTRAQ	http://www.securityfocus.com/bid/84014
BUGTRAQ	http://www.securityfocus.com/bid/84012
BUGTRAQ	http://www.securityfocus.com/bid/84016
BUGTRAQ	http://www.securityfocus.com/bid/84011

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/84022
BUGTRAQ	http://www.securityfocus.com/bid/84009
MSB	http://technet.microsoft.com/security/bulletin/MS16-024
MSB	http://technet.microsoft.com/security/bulletin/MS16-023
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-184
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-023
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-179
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-187
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-180
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-183
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-186
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-188
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-185

MS16-028: Security Update for Microsoft Windows PDF Library to Address Remote Code Execution

High

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-028' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-028'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0117
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0118
BUGTRAQ	http://www.securityfocus.com/bid/84112
BUGTRAQ	http://www.securityfocus.com/bid/84109
MSB	http://technet.microsoft.com/security/bulletin/MS16-028
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-177
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-028

MS16-037: Cumulative Security Update for Internet Explorer — High

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-037' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-

037'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0154
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0159
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0166
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0164
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0162
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0160
BUGTRAQ	http://www.securityfocus.com/bid/85922
BUGTRAQ	http://www.securityfocus.com/bid/85939
MSB	http://technet.microsoft.com/security/bulletin/MS16-037
MSB	http://technet.microsoft.com/security/bulletin/MS16-038
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-231
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-037
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-230
URL	http://packetstormsecurity.com/files/136702/Microsoft-Internet-Explorer-11-DLL-Hijacking.html

MS16-039: Security Update for Microsoft Graphics Component High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-039'.

Affected Products Are:
- Microsoft Live Meeting 2007 Console
- Microsoft Lync 2010 (32-bit)
- Microsoft Lync 2010 (64-bit)
- Microsoft Lync 2010 Attendee (admin level install)
- Microsoft Lync 2010 Attendee (user level install)
- Microsoft Lync 2013
- Microsoft Lync Basic 2013
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office Word Viewer
- Skype
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-039' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0167
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0165
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0143
BUGTRAQ	http://www.securityfocus.com/bid/85896
MSB	http://technet.microsoft.com/security/bulletin/MS16-039
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-039
URL	https://cwe.mitre.org/data/definitions/119.html

MS16-040: Security Update for Microsoft XML Core Services High

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-040' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-040'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7

- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0147
MSB	http://technet.microsoft.com/security/bulletin/MS16-040
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-040

MS16-063: Cumulative Security Update for Internet Explorer — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-063' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-063'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3212
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3213
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3205
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3206
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3207
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3202
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0199
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0200
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3211
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3210
BUGTRAQ	http://www.securityfocus.com/bid/91106
BUGTRAQ	http://www.securityfocus.com/bid/91105
MSB	http://technet.microsoft.com/security/bulletin/MS16-068
MSB	http://technet.microsoft.com/security/bulletin/MS16-069
MSB	http://technet.microsoft.com/security/bulletin/MS16-077
MSB	http://technet.microsoft.com/security/bulletin/MS16-063

Type	Reference
URL	https://cwe.mitre.org/data/definitions/79.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-063
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://packetstormsecurity.com/files/137533/Microsoft-Internet-Explorer-11-Garbage-Collector-Attribute-Type-Confusion.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-365
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-366

MS16-087: Security Update for Windows Print Spooler Components — High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-087'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-087' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.1

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3238
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3239
BUGTRAQ	http://www.securityfocus.com/bid/91609
BUGTRAQ	http://www.securityfocus.com/bid/91612
MSB	http://technet.microsoft.com/security/bulletin/MS16-087
URL	https://cwe.mitre.org/data/definitions/254.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-087

MS16-095: Cumulative Security Update for Internet Explorer — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-095' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-095'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7

- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3327
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3321
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3290
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3288
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3326
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3329
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3289
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3293
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3322
BUGTRAQ	http://www.securityfocus.com/bid/92287
BUGTRAQ	http://www.securityfocus.com/bid/92291
BUGTRAQ	http://www.securityfocus.com/bid/92322
BUGTRAQ	http://www.securityfocus.com/bid/92321
BUGTRAQ	http://www.securityfocus.com/bid/92286
BUGTRAQ	http://www.securityfocus.com/bid/92284
BUGTRAQ	http://www.securityfocus.com/bid/92285
BUGTRAQ	http://www.securityfocus.com/bid/92305
BUGTRAQ	http://www.securityfocus.com/bid/92282

Type	Reference
MSB	https://technet.microsoft.com/library/security/MS16-096
MSB	https://technet.microsoft.com/library/security/MS16-095
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://www.securify.nl/advisory/SFY20160301/internet_explorer_iframe_sandbox_local_file_name_disclosure_vulnerability.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-095

MS16-104: Cumulative Security Update for Internet Explorer High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-104'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-104' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3292
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3295
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3297
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3351
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3325
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3324
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3247
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3353
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3375
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3291
BUGTRAQ	http://www.securityfocus.com/bid/92808
BUGTRAQ	http://www.securityfocus.com/bid/92830
BUGTRAQ	http://www.securityfocus.com/bid/92788
BUGTRAQ	http://www.securityfocus.com/bid/92832
BUGTRAQ	http://www.securityfocus.com/bid/92809
BUGTRAQ	http://www.securityfocus.com/bid/92829
BUGTRAQ	http://www.securityfocus.com/bid/92835
BUGTRAQ	http://www.securityfocus.com/bid/92828
BUGTRAQ	http://www.securityfocus.com/bid/92827
BUGTRAQ	http://www.securityfocus.com/bid/92834
MSB	http://technet.microsoft.com/security/bulletin/MS16-104

Type	Reference
MSB	http://technet.microsoft.com/security/bulletin/MS16-105
MSB	http://technet.microsoft.com/security/bulletin/MS16-116
URL	https://www.brokenbrowser.com/detecting-apps-mimetype-malware/
URL	http://blog.skylined.nl/20161118002.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-104
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://zerodayinitiative.com/advisories/ZDI-16-506/
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html

MS16-116: Security Update in OLE Automation for VBScript Scripting Engine

High

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-116' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-116'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3375
BUGTRAQ	http://www.securityfocus.com/bid/92835
MSB	http://technet.microsoft.com/security/bulletin/MS16-116
MSB	http://technet.microsoft.com/security/bulletin/MS16-104
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-116

MS16-118: Cumulative Security Update for Internet Explorer High

Solution Details

Microsoft has released a fix for this flaw in their October 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-118'.

Affected Products Are:
- Windows 10

- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3267
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3331
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3382
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3387
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3388
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3390
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3391
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3383
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3384
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3385
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3298
BUGTRAQ	http://www.securityfocus.com/bid/93387
BUGTRAQ	http://www.securityfocus.com/bid/93376
BUGTRAQ	http://www.securityfocus.com/bid/93386
BUGTRAQ	http://www.securityfocus.com/bid/93381

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/93382
BUGTRAQ	http://www.securityfocus.com/bid/93383
BUGTRAQ	http://www.securityfocus.com/bid/93379
BUGTRAQ	http://www.securityfocus.com/bid/93396
BUGTRAQ	http://www.securityfocus.com/bid/93393
BUGTRAQ	http://www.securityfocus.com/bid/93397
BUGTRAQ	http://www.securityfocus.com/bid/93392
MSB	http://technet.microsoft.com/security/bulletin/MS16-119
MSB	http://technet.microsoft.com/security/bulletin/MS16-118
MSB	http://technet.microsoft.com/security/bulletin/MS16-126
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-118

MS16-130: Security Update for Microsoft Windows High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-130'.

Affected Products Are:
- Windows 10

- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their November 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7212
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7222
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7221
BUGTRAQ	http://www.securityfocus.com/bid/94027
BUGTRAQ	http://www.securityfocus.com/bid/94023
BUGTRAQ	http://www.securityfocus.com/bid/94021
MSB	http://technet.microsoft.com/security/bulletin/MS16-130
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-130
URL	https://cwe.mitre.org/data/definitions/284.html

MS16-132: Security Update for Microsoft Graphics Component High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-132'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their November 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7210
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7256
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7217
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7205
BUGTRAQ	http://www.securityfocus.com/bid/94030
BUGTRAQ	http://www.securityfocus.com/bid/94033
BUGTRAQ	http://www.securityfocus.com/bid/94156

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/94066
MSB	http://technet.microsoft.com/security/bulletin/MS16-132
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://secuniaresearch.flexerasoftware.com/secunia_research/2016-16/
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-132
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://twitter.com/da5ch0/status/820161895269277696
URL	https://cwe.mitre.org/data/definitions/200.html

MS16-144: Cumulative Security Update for Internet Explorer

High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-144'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their December 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7284
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7279
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7281
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7282
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7287
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7202
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7283
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7278
BUGTRAQ	http://www.securityfocus.com/bid/94719
BUGTRAQ	http://www.securityfocus.com/bid/94723
BUGTRAQ	http://www.securityfocus.com/bid/94724
BUGTRAQ	http://www.securityfocus.com/bid/94722
BUGTRAQ	http://www.securityfocus.com/bid/94042
BUGTRAQ	http://www.securityfocus.com/bid/94725
BUGTRAQ	http://www.securityfocus.com/bid/94726
BUGTRAQ	http://www.securityfocus.com/bid/94716
MSB	http://technet.microsoft.com/security/bulletin/MS16-145
MSB	http://technet.microsoft.com/security/bulletin/MS16-144
MSB	http://technet.microsoft.com/security/bulletin/MS16-129

Type	Reference
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-593
URL	https://bugs.chromium.org/p/project-zero/issues/detail?id=972
URL	http://packetstormsecurity.com/files/140251/Microsoft-Edge-Internationalization-Type-Confusion.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-144
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/254.html

MS16-146: Security Update for Microsoft Graphics Component High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-146'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2

- Windows Server 2012 R2 (server core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their December 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7257
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7272
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7273
BUGTRAQ	http://www.securityfocus.com/bid/94755
BUGTRAQ	http://www.securityfocus.com/bid/94739
BUGTRAQ	http://www.securityfocus.com/bid/94752
MSB	http://technet.microsoft.com/security/bulletin/MS16-148
MSB	http://technet.microsoft.com/security/bulletin/MS16-146
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-645
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-146
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/200.html

MS16-147: Security Update for Microsoft Uniscribe High

Solution Details

Microsoft has released a fix for this flaw in their December 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS16-147'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7274
BUGTRAQ	http://www.securityfocus.com/bid/94758
MSB	http://technet.microsoft.com/security/bulletin/MS16-147
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-147
URL	https://cwe.mitre.org/data/definitions/19.html

MS17-006: Cumulative Security Update for Internet Explorer — High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS17-006'.

Affected Products Are:
- Internet Explorer 10
- Internet Explorer 11
- Internet Explorer 9
- Microsoft Internet Messaging API

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their March 2017 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0037
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0008
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0018
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0040
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0049
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0059
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0012
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0009
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0033
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0130
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0149
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0154

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/96087
BUGTRAQ	http://www.securityfocus.com/bid/96088
BUGTRAQ	http://www.securityfocus.com/bid/96073
BUGTRAQ	http://www.securityfocus.com/bid/96086
BUGTRAQ	http://www.securityfocus.com/bid/96094
BUGTRAQ	http://www.securityfocus.com/bid/96095
BUGTRAQ	http://www.securityfocus.com/bid/96077
BUGTRAQ	http://www.securityfocus.com/bid/96085
BUGTRAQ	http://www.securityfocus.com/bid/96645
BUGTRAQ	http://www.securityfocus.com/bid/96647
BUGTRAQ	http://www.securityfocus.com/bid/96724
BUGTRAQ	http://www.securityfocus.com/bid/96766
URL	http://technet.microsoft.com/en-us/security/bulletin/MS17-006
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0033
URL	https://bugs.chromium.org/p/project-zero/issues/detail?id=1011
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0037
URL	https://0patch.blogspot.si/2017/03/0patching-another-0-day-internet.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0008
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0018
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0040

Type	Reference
URL	http://www.security-assessment.com/files/documents/advisory/reversesegment.pdf
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0009
URL	https://cwe.mitre.org/data/definitions/704.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0012
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0059
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0130
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0149
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0154
URL	https://cwe.mitre.org/data/definitions/74.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html

MS17-010: Security Update for Microsoft Windows SMB Server High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their March 2017 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'ms17-010'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0146
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0144
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0147
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0148
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0143
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0145
BUGTRAQ	http://www.securityfocus.com/bid/96705
BUGTRAQ	http://www.securityfocus.com/bid/96707
BUGTRAQ	http://www.securityfocus.com/bid/96709
BUGTRAQ	http://www.securityfocus.com/bid/96703
BUGTRAQ	http://www.securityfocus.com/bid/96706
BUGTRAQ	http://www.securityfocus.com/bid/96704

Type	Reference
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0145
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0146
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0147
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0148
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0143
URL	https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02
URL	http://technet.microsoft.com/en-us/security/bulletin/ms17-010

MS17-013: Security Update for Microsoft Graphics Component High

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Critical' and released a fix for this in Microsoft Security Bulletin 'MS17-013'.

Affected Products Are:

- Microsoft Live Meeting 2007 Add-in
- Microsoft Live Meeting 2007 Console
- Microsoft Lync 2010 (32-bit)
- Microsoft Lync 2010 (64-bit)
- Microsoft Lync 2010 Attendee (admin level install)
- Microsoft Lync 2010 Attendee (user level install)
- Microsoft Lync 2013
- Microsoft Lync Basic 2013
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows clients
- Microsoft Silverlight 5 Developer Runtime when installed on all supported releases of Microsoft Windows servers
- Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows clients
- Microsoft Silverlight 5 when installed on all supported releases of Microsoft Windows servers
- Microsoft Word Viewer
- Skype
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their March 2017 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0062

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0060
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0108
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0014
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0001
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0005
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0038
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0063
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0061
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0025
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0047
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0073
BUGTRAQ	http://www.securityfocus.com/bid/96643
BUGTRAQ	http://www.securityfocus.com/bid/96713
BUGTRAQ	http://www.securityfocus.com/bid/96034
BUGTRAQ	http://www.securityfocus.com/bid/96023
BUGTRAQ	http://www.securityfocus.com/bid/96013
BUGTRAQ	http://www.securityfocus.com/bid/96057
BUGTRAQ	http://www.securityfocus.com/bid/96033
BUGTRAQ	http://www.securityfocus.com/bid/96722
BUGTRAQ	http://www.securityfocus.com/bid/96638
BUGTRAQ	http://www.securityfocus.com/bid/96626
BUGTRAQ	http://www.securityfocus.com/bid/96637
BUGTRAQ	http://www.securityfocus.com/bid/96715
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0062

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0060
URL	http://technet.microsoft.com/en-us/security/bulletin/MS17-013
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0014
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0108
URL	https://github.com/k0keoyo/CVE-2017-0038-EXP-C-JS
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0038
URL	https://0patch.blogspot.com/2017/02/0patching-0-day-windows-gdi32dll-memory.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0001
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0005
URL	https://bugs.chromium.org/p/project-zero/issues/detail?id=992
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0063
URL	https://blogs.technet.microsoft.com/mmpc/2017/03/27/detecting-and-mitigating-elevation-of-privilege-exploit-for-cve-2017-0005/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0061
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0025
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0047
URL	https://secuniaresearch.flexerasoftware.com/secunia_research/2017-9/
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0073

MS17-APR: Microsoft Internet Explorer Security Update | High

Solution Details

Microsoft has released a fix for this flaw in their April 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-0210 - Internet Explorer Elevation of Privilege Vulnerability
CVE-2017-0202 - Internet Explorer Memory Corruption Vulnerability
CVE-2017-0201 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows Server 2016 (Server Core installation)
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 9 on Windows Vista x64 Edition Service Pack 2
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 9 on Windows Vista Service Pack 2
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0210
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0201
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0202
BUGTRAQ	http://www.securityfocus.com/bid/97512
BUGTRAQ	http://www.securityfocus.com/bid/97454
BUGTRAQ	http://www.securityfocus.com/bid/97441
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0201
URL	https://support.microsoft.com/en-us/help/4015551
URL	https://support.microsoft.com/en-us/help/4015550
URL	https://support.microsoft.com/en-us/help/4015217
URL	https://support.microsoft.com/en-us/help/4015221
URL	https://support.microsoft.com/en-us/help/4015583
URL	https://support.microsoft.com/en-us/help/4015219
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0202
URL	https://support.microsoft.com/en-us/help/4014661
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0210
URL	https://cwe.mitre.org/data/definitions/119.html

MS17-APR: Microsoft .NET Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their April 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released a security update for Microsoft .NET Framework which includes fixes for the following vulnerabilities:

CVE-2017-0160 - .NET Remote Code Execution Vulnerability

Affected Products:
Microsoft .NET Framework 4.5.2 on Windows Vista x64 Edition Service Pack 2
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Vista Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.5.2 on Windows RT 8.1
Microsoft .NET Framework 4.6.2 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 4.6.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.6.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for 32-bit Systems
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.6.2 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 4.6.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6 on Windows Vista Service Pack 2
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6.2 on Windows Server 2012 R2
Microsoft .NET Framework 4.5.2 on Windows Vista Service Pack 2
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6.2 on Windows Server 2012
Microsoft .NET Framework 4.6.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for 32-bit Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1

Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.6.2 on Windows RT 8.1
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows Server 2016
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2012
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Vista x64 Edition Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows Server 2012 R2
Microsoft .NET Framework 4.6/4.6.1 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.6.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2
Microsoft .NET Framework 4.6.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 4.6.2 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 4.6 on Windows 10 for x64-based Systems
Microsoft .NET Framework 4.6.2 on Windows Server 2016
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.6 on Windows Vista x64 Edition Service Pack 2
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2012 R2
Microsoft .NET Framework 4.6/4.6.1 on Windows RT 8.1
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1 on Windows 8.1 for 32-bit systems

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0160
BUGTRAQ	http://www.securityfocus.com/bid/97447
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0160
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://support.microsoft.com/en-us/help/4015583
URL	https://support.microsoft.com/en-us/help/4015217
URL	https://support.microsoft.com/en-us/help/4015219
URL	https://support.microsoft.com/en-us/help/4014984
URL	https://support.microsoft.com/en-us/help/4014983
URL	https://support.microsoft.com/en-us/help/4014982
URL	https://support.microsoft.com/en-us/help/4014981
URL	https://support.microsoft.com/en-us/help/4015221

MS17-APR: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2017-0185 - Hyper-V Denial of Service Vulnerability
CVE-2017-0192 - ATMFD.dll Information Disclosure Vulnerability
CVE-2017-0211 - Windows OLE Elevation of Privilege Vulnerability
CVE-2017-0169 - Hyper-V Information Disclosure Vulnerability
CVE-2017-0058 - Win32k Information Disclosure Vulnerability
CVE-2017-0191 - Windows Denial of Service Vulnerability
CVE-2017-0165 - Windows Elevation of Privilege Vulnerability
CVE-2017-0163 - Hyper-V Remote Code Execution Vulnerability
CVE-2017-0159 - ADFS Security Feature Bypass Vulnerability
CVE-2017-0167 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-0183 - Hyper-V Denial of Service Vulnerability
CVE-2017-0180 - Hyper-V Remote Code Execution Vulnerability
CVE-2017-0158 - Scripting Engine Memory Corruption Vulnerability
CVE-2017-0164 - Active Directory Denial of Service Vulnerability
CVE-2017-0184 - Hyper-V Denial of Service Vulnerability

CVE-2017-0181 - Hyper-V Remote Code Execution Vulnerability
CVE-2017-0162 - Hyper-V Remote Code Execution Vulnerability
CVE-2017-0182 - Hyper-V Denial of Service Vulnerability
CVE-2017-0188 - Win32k Information Disclosure Vulnerability
CVE-2017-0168 - Hyper-V Information Disclosure Vulnerability
CVE-2017-0179 - Hyper-V Denial of Service Vulnerability
CVE-2017-0155 - Windows Graphics Elevation of Privilege Vulnerability
CVE-2017-0189 - Win32k Elevation of Privilege Vulnerability
CVE-2017-0166 - LDAP Elevation of Privilege Vulnerability
CVE-2017-0178 - Hyper-V Denial of Service Vulnerability
CVE-2017-0156 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2017-0186 - Hyper-V Denial of Service Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1511 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1511 for 32-bit Systems
Windows Server 2016 (Server Core installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1703 for x64-based Systems
Windows Vista Service Pack 2
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Server 2016
Windows Vista x64 Edition Service Pack 2
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Solution Details

Microsoft has released a fix for this flaw in their April 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.1

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0186
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0189
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0188
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0167
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0179
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0169
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0155
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0192
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0163
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0211
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0181
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0184
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0166
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0168
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0158
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0058
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0165
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0159
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0191
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0183
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0156

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0162
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0164
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0185
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0180
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0178
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0182
BUGTRAQ	http://www.securityfocus.com/bid/97444
BUGTRAQ	http://www.securityfocus.com/bid/97438
BUGTRAQ	http://www.securityfocus.com/bid/97420
BUGTRAQ	http://www.securityfocus.com/bid/97475
BUGTRAQ	http://www.securityfocus.com/bid/97473
BUGTRAQ	http://www.securityfocus.com/bid/97426
BUGTRAQ	http://www.securityfocus.com/bid/97459
BUGTRAQ	http://www.securityfocus.com/bid/97471
BUGTRAQ	http://www.securityfocus.com/bid/97452
BUGTRAQ	http://www.securityfocus.com/bid/97465
BUGTRAQ	http://www.securityfocus.com/bid/97514
BUGTRAQ	http://www.securityfocus.com/bid/97445
BUGTRAQ	http://www.securityfocus.com/bid/97435
BUGTRAQ	http://www.securityfocus.com/bid/97446
BUGTRAQ	http://www.securityfocus.com/bid/97418
BUGTRAQ	http://www.securityfocus.com/bid/97455
BUGTRAQ	http://www.securityfocus.com/bid/97462
BUGTRAQ	http://www.securityfocus.com/bid/97467

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/97449
BUGTRAQ	http://www.securityfocus.com/bid/97466
BUGTRAQ	http://www.securityfocus.com/bid/97428
BUGTRAQ	http://www.securityfocus.com/bid/97507
BUGTRAQ	http://www.securityfocus.com/bid/97461
BUGTRAQ	http://www.securityfocus.com/bid/97448
BUGTRAQ	http://www.securityfocus.com/bid/97437
BUGTRAQ	http://www.securityfocus.com/bid/97416
BUGTRAQ	http://www.securityfocus.com/bid/97427
URL	https://support.microsoft.com/en-us/help/4015583
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0186
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0189
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0188
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0167
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0179
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0169
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0155
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0192

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0163
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0211
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0181
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0184
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0166
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0168
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0158
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0058
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0165
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0159
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0191
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0183
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0156
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0162
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0164
URL	https://support.microsoft.com/en-us/help/3211308

Type	Reference
URL	https://support.microsoft.com/en-us/help/4015067
URL	https://support.microsoft.com/en-us/help/4015068
URL	https://support.microsoft.com/en-us/help/4015549
URL	https://support.microsoft.com/en-us/help/4015195
URL	https://support.microsoft.com/en-us/help/3217841
URL	https://support.microsoft.com/en-us/help/4015380
URL	https://support.microsoft.com/en-us/help/4015221
URL	https://support.microsoft.com/en-us/help/4015551
URL	https://support.microsoft.com/en-us/help/4015550
URL	https://support.microsoft.com/en-us/help/4015219
URL	https://support.microsoft.com/en-us/help/4015217
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0185
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0180
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0178
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0182
URL	https://cwe.mitre.org/data/definitions/20.html

MS17-AUG: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2017-8591 - Windows IME Remote Code Execution Vulnerability
CVE-2017-8593 - Win32k Elevation of Privilege Vulnerability

CVE-2017-8654 - Microsoft Office SharePoint XSS Vulnerability
CVE-2017-0174 - Windows NetBIOS Denial of Service Vulnerability
CVE-2017-0250 - Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2017-0293 - Windows PDF Remote Code Execution Vulnerability
CVE-2017-8620 - Windows Search Remote Code Execution Vulnerability
CVE-2017-8622 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2017-8623 - Windows Hyper-V Denial of Service Vulnerability
CVE-2017-8624 - Windows CLFS Elevation of Privilege Vulnerability
CVE-2017-8627 - Windows Subsystem for Linux Denial of Service Vulnerability
CVE-2017-8633 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2017-8664 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2017-8666 - Win32k Information Disclosure Vulnerability
CVE-2017-8668 - Volume Manager Extension Driver Information Disclosure Vulnerability
CVE-2017-8673 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2017-8691 - Express Compressed Fonts Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1511 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1511 for 32-bit Systems
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Microsoft SharePoint Server 2010 Service Pack 2
Windows Server 2016
Windows 8.1 for 32-bit systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Solution Details

Microsoft has released a fix for this flaw in their August 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8673
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8624
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8627
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8691
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8664
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8620
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8593
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0250
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8666
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8591
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8668
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8622
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8633
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8623
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0293
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0174
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8654
BUGTRAQ	http://www.securityfocus.com/bid/100064
BUGTRAQ	http://www.securityfocus.com/bid/100079
BUGTRAQ	http://www.securityfocus.com/bid/100061

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/100065
BUGTRAQ	http://www.securityfocus.com/bid/100090
BUGTRAQ	http://www.securityfocus.com/bid/100085
BUGTRAQ	http://www.securityfocus.com/bid/100034
BUGTRAQ	http://www.securityfocus.com/bid/100032
BUGTRAQ	http://www.securityfocus.com/bid/98100
BUGTRAQ	http://www.securityfocus.com/bid/100089
BUGTRAQ	http://www.securityfocus.com/bid/99430
BUGTRAQ	http://www.securityfocus.com/bid/100092
BUGTRAQ	http://www.securityfocus.com/bid/100040
BUGTRAQ	http://www.securityfocus.com/bid/100069
BUGTRAQ	http://www.securityfocus.com/bid/100042
BUGTRAQ	http://www.securityfocus.com/bid/100039
BUGTRAQ	http://www.securityfocus.com/bid/100038
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8624
URL	https://support.microsoft.com/en-us/help/4035056
URL	https://support.microsoft.com/en-us/help/4034666
URL	https://support.microsoft.com/en-us/help/2956077
URL	https://support.microsoft.com/en-us/help/4034034
URL	https://support.microsoft.com/en-us/help/4034679
URL	https://support.microsoft.com/en-us/help/4034674
URL	https://support.microsoft.com/en-us/help/4034775
URL	https://support.microsoft.com/en-us/help/4035055
URL	https://support.microsoft.com/en-us/help/4035679

Type	Reference
URL	https://support.microsoft.com/en-us/help/4034672
URL	https://support.microsoft.com/en-us/help/4034664
URL	https://support.microsoft.com/en-us/help/4034744
URL	https://support.microsoft.com/en-us/help/4034745
URL	https://support.microsoft.com/en-us/help/4022750
URL	https://support.microsoft.com/en-us/help/4034660
URL	https://support.microsoft.com/en-us/help/4034665
URL	https://support.microsoft.com/en-us/help/4034668
URL	https://support.microsoft.com/en-us/help/4034658
URL	https://support.microsoft.com/en-us/help/4034681
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8673
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8627
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8691
URL	https://fortiguard.com/zeroday/FG-VD-17-142
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8664
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8620
URL	https://threatpost.com/windows-search-bug-worth-watching-and-squashing/127434/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8593
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8666
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8591

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8668
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8622
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8633
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8623
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0293
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0250
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0174
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8654
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html

MS17-DEC: Microsoft Internet Explorer Security Update High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-11890 - Scripting Engine Memory Corruption Vulnerability
CVE-2017-11901 - Scripting Engine Memory Corruption Vulnerability

CVE-2017-11903 - Scripting Engine Memory Corruption Vulnerability
CVE-2017-11906 - Scripting Engine Information Disclosure Vulnerability
CVE-2017-11913 - Scripting Engine Memory Corruption Vulnerability
CVE-2017-11930 - Scripting Engine Memory Corruption Vulnerability
CVE-2017-11886 - Scripting Engine Memory Corruption Vulnerability
CVE-2017-11887 - Scripting Engine Information Disclosure Vulnerability
CVE-2017-11907 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
ChakraCore
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

Solution Details

Microsoft has released a fix for this flaw in their December 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11906
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11886
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11913
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11907

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11887
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11890
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11930
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11901
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11903
BUGTRAQ	http://www.securityfocus.com/bid/102078
BUGTRAQ	http://www.securityfocus.com/bid/102062
BUGTRAQ	http://www.securityfocus.com/bid/102091
BUGTRAQ	http://www.securityfocus.com/bid/102045
BUGTRAQ	http://www.securityfocus.com/bid/102063
BUGTRAQ	http://www.securityfocus.com/bid/102082
BUGTRAQ	http://www.securityfocus.com/bid/102058
BUGTRAQ	http://www.securityfocus.com/bid/102046
BUGTRAQ	http://www.securityfocus.com/bid/102047
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11906
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11886
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11913
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11907
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11887
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11890

Type	Reference
URL	https://support.microsoft.com/en-us/help/4052978
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11930
URL	https://support.microsoft.com/en-us/help/4054518
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11901
URL	https://support.microsoft.com/en-us/help/4053578
URL	https://support.microsoft.com/en-us/help/4054520
URL	https://support.microsoft.com/en-us/help/4053579
URL	https://support.microsoft.com/en-us/help/4054519
URL	https://support.microsoft.com/en-us/help/4053581
URL	https://support.microsoft.com/en-us/help/4053580
URL	https://support.microsoft.com/en-us/help/4054517
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11903

MS17-DEC: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their December 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2017-11885 - Windows RRAS Service Remote Code Execution Vulnerability
CVE-2017-11899 - Microsoft Windows Security Feature Bypass Vulnerability
CVE-2017-11927 - Microsoft Windows Information Disclosure Vulnerability
CVE-2017-11932 - Microsoft Exchange Spoofing Vulnerability
CVE-2017-11937 - Microsoft Malware Protection Engine Remote Code Execution Vulnerability
ADV170023 - Microsoft Exchange Defense in Depth Update
CVE-2017-11916 - Scripting Engine Memory Corruption Vulnerability

CVE-2017-11936 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2017-11940 - Microsoft Malware Protection Engine Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Exchange Server 2013 Cumulative Update 18
Microsoft Forefront Endpoint Protection 2010
Microsoft Exchange Server 2016 Cumulative Update 7
Windows 10 for 32-bit Systems
Windows Defender on Windows 8.1 for 32-bit systems
Microsoft Exchange Server 2016
Microsoft SharePoint Enterprise Server 2016
Microsoft Exchange Server 2013
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Defender on Windows 10 Version 1511 for x64-based Systems
Windows Server 2012 (Server Core installation)
Windows Defender on Windows 10 Version 1703 for x64-based Systems
Windows Server 2012
Windows Defender on Windows Server 2016 (Server Core installation)
Windows 7 for x64-based Systems Service Pack 1
Windows Defender on Windows 10 Version 1607 for 32-bit Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for x64-based Systems
Windows Defender on Windows Server 2016
Windows Intune Endpoint Protection
Windows 8.1 for x64-based systems
Windows Defender on Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2012 R2
ChakraCore
Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1607 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for 32-bit Systems
Microsoft Exchange Server 2016 Cumulative Update 6
Windows Defender on Windows 8.1 for x64-based systems
Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft Exchange Server 2013 Cumulative Update 17
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1511 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1

Windows 7 for 32-bit Systems Service Pack 1
Microsoft Security Essentials
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Microsoft System Center Endpoint Protection
Windows Defender on Windows 10 Version 1511 for 32-bit Systems
Windows Defender on Windows 10 for 32-bit Systems
Windows Defender on Windows 10 for x64-based Systems
Windows Server 2016
Windows Defender on Windows 10 Version 1703 for 32-bit Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows 7 for x64-based Systems Service Pack 1
Windows Defender on Windows Server, version 1709 (Server Core Installation)
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11937
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11885
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11940
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11927
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11899
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11916
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11932
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11936
BUGTRAQ	http://www.securityfocus.com/bid/102055
BUGTRAQ	http://www.securityfocus.com/bid/102068
BUGTRAQ	http://www.securityfocus.com/bid/102104
BUGTRAQ	http://www.securityfocus.com/bid/102095

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/102077
BUGTRAQ	http://www.securityfocus.com/bid/102090
BUGTRAQ	http://www.securityfocus.com/bid/102060
BUGTRAQ	http://www.securityfocus.com/bid/102070
URL	https://support.microsoft.com/en-us/help/4054519
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11937
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11885
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11936
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11940
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11927
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11899
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11916
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11932
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://support.microsoft.com/en-us/help/4054522
URL	https://support.microsoft.com/en-us/help/4053473
URL	https://support.microsoft.com/en-us/help/4054521

Type	Reference
URL	https://support.microsoft.com/en-us/help/4045655
URL	https://support.microsoft.com/en-us/help/4054523
URL	https://support.microsoft.com/en-us/help/4011576
URL	https://support.microsoft.com/en-us/help/4052303
URL	https://support.microsoft.com/en-us/help/4054517
URL	https://support.microsoft.com/en-us/help/4053580
URL	https://support.microsoft.com/en-us/help/4053581
URL	https://support.microsoft.com/en-us/help/4053579
URL	https://support.microsoft.com/en-us/help/4054520
URL	https://support.microsoft.com/en-us/help/4053578
URL	https://support.microsoft.com/en-us/help/4054518

MS17-JUL: Microsoft Internet Explorer Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-8594 - Internet Explorer Memory Corruption Vulnerability
CVE-2017-8618 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows Server 2012 R2

Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

Solution Details

Microsoft has released a fix for this flaw in their July 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8618
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8594
BUGTRAQ	http://www.securityfocus.com/bid/99399
BUGTRAQ	http://www.securityfocus.com/bid/99401
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8618
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8594
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4025339
URL	https://support.microsoft.com/en-us/help/4025342
URL	https://support.microsoft.com/en-us/help/4025252
URL	https://support.microsoft.com/en-us/help/4025331
URL	https://support.microsoft.com/en-us/help/4025336
URL	https://support.microsoft.com/en-us/help/4025338
URL	https://support.microsoft.com/en-us/help/4025344

Type	Reference
URL	https://support.microsoft.com/en-us/help/4025341

MS17-JUL: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2017-8569 - SharePoint Server XSS Vulnerability
CVE-2017-8573 - Microsoft Graphics Component Elevation of Privilege Vulnerability
CVE-2017-8574 - Microsoft Graphics Component Elevation of Privilege Vulnerability
CVE-2017-8577 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8578 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8580 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8581 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8582 - Https.sys Information Disclosure Vulnerability
CVE-2017-8584 - HoloLens Remote Code Execution Vulnerability
CVE-2017-8587 - Windows Explorer Denial of Service Vulnerability
CVE-2017-8588 - WordPad Remote Code Execution Vulnerability
CVE-2017-8589 - Windows Search Remote Code Execution Vulnerability
CVE-2017-8590 - Windows CLFS Elevation of Privilege Vulnerability
CVE-2017-8621 - Microsoft Exchange Open Redirect Vulnerability
CVE-2017-0170 - Windows Performance Monitor Information Disclosure Vulnerability
CVE-2017-8463 - Windows Explorer Remote Code Execution Vulnerability
CVE-2017-8467 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8486 - Win32k Information Disclosure Vulnerability
CVE-2017-8495 - Kerberos SNAME Security Feature Bypass Vulnerability
CVE-2017-8556 - Microsoft Graphics Component Elevation of Privilege Vulnerability
CVE-2017-8557 - Windows System Information Console Information Disclosure Vulnerability
CVE-2017-8560 - Microsoft Exchange Cross-Site Scripting Vulnerability
CVE-2017-8559 - Microsoft Exchange Cross-Site Scripting Vulnerability
CVE-2017-8561 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2017-8562 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2017-8563 - Windows Elevation of Privilege Vulnerability
CVE-2017-8564 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8565 - Windows PowerShell Remote Code Execution Vulnerability
CVE-2017-8566 - Windows IME Elevation of Privilege Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft SharePoint Enterprise Server 2016
Windows Server 2012 (Server Core installation)

Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Microsoft Exchange Server 2013 Service Pack 1
Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft Exchange Server 2013 Cumulative Update 16
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1511 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Microsoft Exchange Server 2010 Service Pack 3
Microsoft Exchange Server 2016 Cumulative Update 5
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their July 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8584
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8562
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8578
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8563
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8486

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8577
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8587
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8582
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8588
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8495
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8560
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8573
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8589
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8463
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8559
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0170
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8590
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8581
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8565
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8574
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8557
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8564
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8569
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8621
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8467
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8566
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8556
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8561
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8580

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/99434
BUGTRAQ	http://www.securityfocus.com/bid/99397
BUGTRAQ	http://www.securityfocus.com/bid/99419
BUGTRAQ	http://www.securityfocus.com/bid/99402
BUGTRAQ	http://www.securityfocus.com/bid/99414
BUGTRAQ	http://www.securityfocus.com/bid/99416
BUGTRAQ	http://www.securityfocus.com/bid/99413
BUGTRAQ	http://www.securityfocus.com/bid/99429
BUGTRAQ	http://www.securityfocus.com/bid/99400
BUGTRAQ	http://www.securityfocus.com/bid/99424
BUGTRAQ	http://www.securityfocus.com/bid/99449
BUGTRAQ	http://www.securityfocus.com/bid/99431
BUGTRAQ	http://www.securityfocus.com/bid/99425
BUGTRAQ	http://www.securityfocus.com/bid/99389
BUGTRAQ	http://www.securityfocus.com/bid/99448
BUGTRAQ	http://www.securityfocus.com/bid/99427
BUGTRAQ	http://www.securityfocus.com/bid/99423
BUGTRAQ	http://www.securityfocus.com/bid/99394
BUGTRAQ	http://www.securityfocus.com/bid/99438
BUGTRAQ	http://www.securityfocus.com/bid/99387
BUGTRAQ	http://www.securityfocus.com/bid/99398
BUGTRAQ	http://www.securityfocus.com/bid/99428
BUGTRAQ	http://www.securityfocus.com/bid/99447
BUGTRAQ	http://www.securityfocus.com/bid/99533

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/99409
BUGTRAQ	http://www.securityfocus.com/bid/99404
BUGTRAQ	http://www.securityfocus.com/bid/99439
BUGTRAQ	http://www.securityfocus.com/bid/99426
BUGTRAQ	http://www.securityfocus.com/bid/99421
URL	https://support.microsoft.com/en-us/help/4022748
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/611.html
URL	https://www.orpheus-lyre.info/
URL	https://cwe.mitre.org/data/definitions/601.html
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8584
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8562
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8578
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8563
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8486
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8577
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8587
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8582
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8588

Type	Reference
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8495
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8560
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8573
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8589
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8463
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8559
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-0170
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8590
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8581
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8565
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8574
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8557
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8564
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8569
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8621
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8467

Type	Reference
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8566
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8556
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8561
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2017-8580
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://support.microsoft.com/en-us/help/4022746
URL	https://support.microsoft.com/en-us/help/4025333
URL	https://support.microsoft.com/en-us/help/4026059
URL	https://support.microsoft.com/en-us/help/4032955
URL	https://support.microsoft.com/en-us/help/4025872
URL	https://support.microsoft.com/en-us/help/4022914
URL	https://support.microsoft.com/en-us/help/4025877
URL	https://support.microsoft.com/en-us/help/4025674
URL	https://support.microsoft.com/en-us/help/3213544
URL	https://support.microsoft.com/en-us/help/4025398
URL	https://support.microsoft.com/en-us/help/4025343
URL	https://support.microsoft.com/en-us/help/4025337
URL	https://support.microsoft.com/en-us/help/4026061
URL	https://support.microsoft.com/en-us/help/4025397
URL	https://support.microsoft.com/en-us/help/4025409

Type	Reference
URL	https://support.microsoft.com/en-us/help/4025339
URL	https://support.microsoft.com/en-us/help/4025342
URL	https://support.microsoft.com/en-us/help/4025331
URL	https://support.microsoft.com/en-us/help/4025336
URL	https://support.microsoft.com/en-us/help/4025338
URL	https://support.microsoft.com/en-us/help/4025344
URL	https://support.microsoft.com/en-us/help/4025341
URL	https://support.microsoft.com/en-us/help/4025497
URL	https://support.microsoft.com/en-us/help/4018588

MS17-JUN: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their June 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2017-0193 - Hypervisor Code Integrity Elevation of Privilege Vulnerability
CVE-2017-8514 - Microsoft SharePoint Reflective XSS Vulnerability
CVE-2017-8551 - Microsoft SharePoint XSS vulnerability
CVE-2017-0173 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2017-0215 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2017-0216 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2017-0218 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2017-0219 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2017-0291 - Windows PDF Remote Code Execution Vulnerability
CVE-2017-0294 - Windows Remote Code Execution Vulnerability
CVE-2017-0295 - Windows Default Folder Tampering Vulnerability
CVE-2017-0296 - Windows TDX Elevation of Privilege Vulnerability
CVE-2017-0297 - Windows Kernel Elevation of Privilege Vulnerability

CVE-2017-0298 - Windows COM Session Elevation of Privilege Vulnerability
CVE-2017-0299 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-0300 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8460 - Windows PDF Information Disclosure Vulnerability
CVE-2017-8462 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8464 - LNK Remote Code Execution Vulnerability
CVE-2017-8465 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8466 - Windows Cursor Elevation of Privilege Vulnerability
CVE-2017-8468 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8469 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8470 - Win32k Information Disclosure Vulnerability
CVE-2017-8471 - Win32k Information Disclosure Vulnerability
CVE-2017-8472 - Win32k Information Disclosure Vulnerability
CVE-2017-8473 - Win32k Information Disclosure Vulnerability
CVE-2017-8474 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8475 - Win32k Information Disclosure Vulnerability
CVE-2017-8476 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8477 - Win32k Information Disclosure Vulnerability
CVE-2017-8478 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8479 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8480 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8481 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8482 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8483 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8484 - Win32k Information Disclosure Vulnerability
CVE-2017-8485 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8488 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8489 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8490 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8491 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8492 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8493 - Windows Security Feature Bypass Vulnerability
CVE-2017-8494 - Windows Elevation of Privilege Vulnerability
CVE-2017-8515 - Windows VAD Cloning Denial of Service Vulnerability
CVE-2017-8544 - Windows Search Information Disclosure Vulnerability
CVE-2017-8543 - Windows Search Remote Code Execution Vulnerability
ADV170008 - Defense-in-depth Update for Microsoft SharePoint
CVE-2017-8553 - GDI Information Disclosure Vulnerablity

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft SharePoint Enterprise Server 2016
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 1

Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Microsoft Project Server 2013 Service Pack 1
Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1511 for 32-bit Systems
Windows Server 2016 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0218
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8478
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8471
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8493
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8492
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8466
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0298
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8469
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8488
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0299
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0193

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0216
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0300
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8543
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0173
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8483
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8479
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0297
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8485
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8470
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0219
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8484
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8514
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8465
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0296
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8460
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8462
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8551
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8482
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0291
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8477
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8472
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0294
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8481
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8464

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8553
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8491
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8494
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8544
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8515
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8468
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8490
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0295
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0215
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8489
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8476
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8473
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8475
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8480
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8474
BUGTRAQ	http://www.securityfocus.com/bid/98833
BUGTRAQ	http://www.securityfocus.com/bid/98849
BUGTRAQ	http://www.securityfocus.com/bid/98845
BUGTRAQ	http://www.securityfocus.com/bid/98896
BUGTRAQ	http://www.securityfocus.com/bid/98850
BUGTRAQ	http://www.securityfocus.com/bid/98842
BUGTRAQ	http://www.securityfocus.com/bid/98844
BUGTRAQ	http://www.securityfocus.com/bid/98841
BUGTRAQ	http://www.securityfocus.com/bid/98870

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/98864
BUGTRAQ	http://www.securityfocus.com/bid/98884
BUGTRAQ	http://www.securityfocus.com/bid/98878
BUGTRAQ	http://www.securityfocus.com/bid/98901
BUGTRAQ	http://www.securityfocus.com/bid/98824
BUGTRAQ	http://www.securityfocus.com/bid/98873
BUGTRAQ	http://www.securityfocus.com/bid/98859
BUGTRAQ	http://www.securityfocus.com/bid/98856
BUGTRAQ	http://www.securityfocus.com/bid/98840
BUGTRAQ	http://www.securityfocus.com/bid/98860
BUGTRAQ	http://www.securityfocus.com/bid/98848
BUGTRAQ	http://www.securityfocus.com/bid/98898
BUGTRAQ	http://www.securityfocus.com/bid/98847
BUGTRAQ	http://www.securityfocus.com/bid/98846
BUGTRAQ	http://www.securityfocus.com/bid/98843
BUGTRAQ	http://www.securityfocus.com/bid/98839
BUGTRAQ	http://www.securityfocus.com/bid/98887
BUGTRAQ	http://www.securityfocus.com/bid/98900
BUGTRAQ	http://www.securityfocus.com/bid/98913
BUGTRAQ	http://www.securityfocus.com/bid/98858
BUGTRAQ	http://www.securityfocus.com/bid/98835
BUGTRAQ	http://www.securityfocus.com/bid/98854
BUGTRAQ	http://www.securityfocus.com/bid/98851
BUGTRAQ	http://www.securityfocus.com/bid/98837

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/98862
BUGTRAQ	http://www.securityfocus.com/bid/98818
BUGTRAQ	http://www.securityfocus.com/bid/98940
BUGTRAQ	http://www.securityfocus.com/bid/98869
BUGTRAQ	http://www.securityfocus.com/bid/98855
BUGTRAQ	http://www.securityfocus.com/bid/98826
BUGTRAQ	http://www.securityfocus.com/bid/98897
BUGTRAQ	http://www.securityfocus.com/bid/98902
BUGTRAQ	http://www.securityfocus.com/bid/98867
BUGTRAQ	http://www.securityfocus.com/bid/98904
BUGTRAQ	http://www.securityfocus.com/bid/98879
BUGTRAQ	http://www.securityfocus.com/bid/98865
BUGTRAQ	http://www.securityfocus.com/bid/98903
BUGTRAQ	http://www.securityfocus.com/bid/98852
BUGTRAQ	http://www.securityfocus.com/bid/98831
BUGTRAQ	http://www.securityfocus.com/bid/98853
BUGTRAQ	http://www.securityfocus.com/bid/98857
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0218
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8515
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8471
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8478
URL	https://support.microsoft.com/en-us/help/4022715

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8493
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8492
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8466
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0298
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8469
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8488
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0299
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0193
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0216
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0300
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8543
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0173
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8483
URL	https://support.microsoft.com/en-us/help/4022887
URL	https://support.microsoft.com/en-us/help/4022717
URL	https://support.microsoft.com/en-us/help/4024402
URL	https://support.microsoft.com/en-us/help/4022013

Type	Reference
URL	https://support.microsoft.com/en-us/help/3203387
URL	https://support.microsoft.com/en-us/help/4022008
URL	https://support.microsoft.com/en-us/help/4021923
URL	https://support.microsoft.com/en-us/help/4022010
URL	https://support.microsoft.com/en-us/help/3217845
URL	https://support.microsoft.com/en-us/help/4022883
URL	https://support.microsoft.com/en-us/help/4021903
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8479
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0297
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8485
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8470
URL	https://support.microsoft.com/en-us/help/3203432
URL	https://support.microsoft.com/en-us/help/4022722
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0219
URL	https://support.microsoft.com/en-us/help/3203399
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8484
URL	https://support.microsoft.com/en-us/help/4022718
URL	https://support.microsoft.com/en-us/help/4022724
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8465

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0296
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8460
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8462
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8551
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8482
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0291
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8477
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8472
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0294
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8481
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8464
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8553
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8491
URL	https://support.microsoft.com/en-us/help/4022727
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8494
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8544

Type	Reference
URL	https://support.microsoft.com/en-us/help/4022726
URL	https://support.microsoft.com/en-us/help/4022719
URL	https://support.microsoft.com/en-us/help/4022725
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8468
URL	https://support.microsoft.com/en-us/help/4022714
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8490
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0295
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0215
URL	https://posts.specterops.io/umci-bypass-using-psworkflowutility-cve-2017-0215-71c76c1588f9
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8489
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8476
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8473
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8475
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8514
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8480

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8474

MS17-MAY: Microsoft Internet Explorer Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their May 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-0064 - Internet Explorer Security Feature Bypass Vulnerability
CVE-2017-0222 - Internet Explorer Memory Corruption Vulnerability
CVE-2017-0226 - Microsoft Internet Explorer Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0226
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0064
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0222
BUGTRAQ	http://www.securityfocus.com/bid/98121
BUGTRAQ	http://www.securityfocus.com/bid/98127
BUGTRAQ	http://www.securityfocus.com/bid/98139
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0226
URL	https://support.microsoft.com/en-us/help/4019474
URL	https://support.microsoft.com/en-us/help/4019472
URL	https://support.microsoft.com/en-us/help/4016871
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://support.microsoft.com/en-us/help/4019215
URL	https://support.microsoft.com/en-us/help/4018271
URL	https://support.microsoft.com/en-us/help/4019214
URL	https://support.microsoft.com/en-us/help/4019473
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0222
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0064
URL	https://support.microsoft.com/en-us/help/4019264

MS17-MAY: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2017-0190 - Windows GDI Information Disclosure Vulnerability
CVE-2017-0077 - Dxgkrnl.sys Elevation of Privilege Vulnerability
CVE-2017-0242 - Microsoft ActiveX Information Disclosure Vulnerability
CVE-2017-0244 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2017-0245 - Win32k Information Disclosure Vulnerability
CVE-2017-0246 - Win32k Elevation of Privilege Vulnerability
CVE-2017-0255 - Microsoft SharePoint XSS Vulnerability
CVE-2017-0258 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-0259 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-0263 - Win32k Elevation of Privilege Vulnerability
CVE-2017-0290 - Microsoft Malware Protection Engine Remote Code Execution Vulnerability
CVE-2017-0171 - Windows DNS Server Denial of Service Vulnerability
CVE-2017-0175 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-0212 - Windows Hyper-V vSMB Elevation of Privilege Vulnerability
CVE-2017-0213 - Windows COM Elevation of Privilege Vulnerability
CVE-2017-0214 - Windows COM Elevation of Privilege Vulnerability
CVE-2017-0220 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-0267 - Windows SMB Information Disclosure Vulnerability
CVE-2017-0268 - Windows SMB Information Disclosure Vulnerability
CVE-2017-0269 - Windows SMB Denial of Service Vulnerability
CVE-2017-0270 - Windows SMB Information Disclosure Vulnerability
CVE-2017-0271 - Windows SMB Information Disclosure Vulnerability
CVE-2017-0272 - Windows SMB Remote Code Execution Vulnerability
CVE-2017-0273 - Windows SMB Denial of Service Vulnerability
CVE-2017-0274 - Windows SMB Information Disclosure Vulnerability
CVE-2017-0275 - Windows SMB Information Disclosure Vulnerability
CVE-2017-0276 - Windows SMB Information Disclosure Vulnerability
CVE-2017-0277 - Windows SMB Remote Code Execution Vulnerability
CVE-2017-0278 - Windows SMB Remote Code Execution Vulnerability
CVE-2017-0279 - Windows SMB Remote Code Execution Vulnerability
CVE-2017-0280 - Windows SMB Denial of Service Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Forefront Security for SharePoint Service Pack 3
Microsoft Forefront Endpoint Protection 2010
Windows 10 for 32-bit Systems
Windows Defender on Windows 8.1 for 32-bit systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Defender on Windows 10 Version 1511 for x64-based Systems
Windows Server 2012 (Server Core installation)
Windows Defender on Windows 10 Version 1703 for x64-based Systems
Windows Server 2012
Windows Defender on Windows Server 2016 (Server Core installation)
Windows 7 for x64-based Systems Service Pack 1
Windows Defender on Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems

Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Defender on Windows Server 2016
Windows Intune Endpoint Protection
Windows 8.1 for x64-based systems
Windows Defender on Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1607 for x64-based Systems
Windows Defender on Windows 8.1 for x64-based systems
Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1511 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows Defender on Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Microsoft Security Essentials
Microsoft SharePoint Foundation 2013 Service Pack 1
Windows Defender on Windows 10 Version 1511 for 32-bit Systems
Windows Defender on Windows 10 for 32-bit Systems
Windows Defender on Windows 10 for x64-based Systems
Windows Server 2016
Windows Defender on Windows 10 Version 1703 for 32-bit Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows 7 for x64-based Systems Service Pack 1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their May 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.1

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0275
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0171

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0273
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0258
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0242
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0255
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0276
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0290
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0270
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0267
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0175
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0244
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0263
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0268
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0279
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0280
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0245
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0259
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0274
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0220
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0077
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0269
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0278
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0271
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0272
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0213

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0212
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0246
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0277
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0190
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0214
BUGTRAQ	http://www.securityfocus.com/bid/98271
BUGTRAQ	http://www.securityfocus.com/bid/98267
BUGTRAQ	http://www.securityfocus.com/bid/98114
BUGTRAQ	http://www.securityfocus.com/bid/98112
BUGTRAQ	http://www.securityfocus.com/bid/98275
BUGTRAQ	http://www.securityfocus.com/bid/98097
BUGTRAQ	http://www.securityfocus.com/bid/98258
BUGTRAQ	http://www.securityfocus.com/bid/98111
BUGTRAQ	http://www.securityfocus.com/bid/98268
BUGTRAQ	http://www.securityfocus.com/bid/98115
BUGTRAQ	http://www.securityfocus.com/bid/98261
BUGTRAQ	http://www.securityfocus.com/bid/98274
BUGTRAQ	http://www.securityfocus.com/bid/98330
BUGTRAQ	http://www.securityfocus.com/bid/98108
BUGTRAQ	http://www.securityfocus.com/bid/98273
BUGTRAQ	http://www.securityfocus.com/bid/98102
BUGTRAQ	http://www.securityfocus.com/bid/98259
BUGTRAQ	http://www.securityfocus.com/bid/98263
BUGTRAQ	http://www.securityfocus.com/bid/98266

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/98264
BUGTRAQ	http://www.securityfocus.com/bid/98265
BUGTRAQ	http://www.securityfocus.com/bid/98270
BUGTRAQ	http://www.securityfocus.com/bid/98260
BUGTRAQ	http://www.securityfocus.com/bid/98113
BUGTRAQ	http://www.securityfocus.com/bid/98298
BUGTRAQ	http://www.securityfocus.com/bid/98107
BUGTRAQ	http://www.securityfocus.com/bid/98110
BUGTRAQ	http://www.securityfocus.com/bid/98272
BUGTRAQ	http://www.securityfocus.com/bid/98109
BUGTRAQ	http://www.securityfocus.com/bid/98099
BUGTRAQ	http://www.securityfocus.com/bid/98103
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0275
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0171
URL	https://support.microsoft.com/en-us/help/4019204
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0220
URL	https://arstechnica.com/information-technology/2017/05/windows-defender-nscript-remote-vulnerability/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0268
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0258
URL	https://support.microsoft.com/en-us/help/4018821
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0242

Type	Reference
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4019264
URL	https://support.microsoft.com/en-us/help/4019473
URL	https://support.microsoft.com/en-us/help/4019214
URL	https://support.microsoft.com/en-us/help/4019149
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0276
URL	https://bugs.chromium.org/p/project-zero/issues/detail?id=1252
URL	https://technet.microsoft.com/library/security/4022344
URL	https://support.microsoft.com/en-us/help/4019206
URL	https://twitter.com/natashenka/status/861748397409058816
URL	https://support.microsoft.com/en-us/help/4019215
URL	https://support.microsoft.com/en-us/help/4016871
URL	https://support.microsoft.com/en-us/help/4019472
URL	https://support.microsoft.com/en-us/help/4019474
URL	https://support.microsoft.com/en-us/help/3191914
URL	https://support.microsoft.com/en-us/help/4018196
URL	https://support.microsoft.com/en-us/help/4018556
URL	https://support.microsoft.com/en-us/help/4018466
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0213
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0270
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0175
URL	https://xiaodaozhi.com/exploit/117.html

Type	Reference
URL	https://0patch.blogspot.si/2017/05/0patching-worst-windows-remote-code.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0212
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0267
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0277
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0280
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0279
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0259
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0245
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.microsoft.com/en-us/help/4018927
URL	https://support.microsoft.com/en-us/help/4018885
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0269
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0077
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0274
URL	https://cwe.mitre.org/data/definitions/79.html

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0278
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0271
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0246
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0272
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0273
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0255
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0190
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0263
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0290
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0244
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0214

MS17-NOV: Microsoft Internet Explorer Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their November 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-11856 - Internet Explorer Memory Corruption Vulnerability
CVE-2017-11834 - Scripting Engine Information Disclosure Vulnerability
CVE-2017-11848 - Internet Explorer Information Disclosure Vulnerability

CVE-2017-11855 - Internet Explorer Memory Corruption Vulnerability
CVE-2017-11869 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1709 for 64-based Systems
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows Server, version 1709 (Server Core Installation)
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11856
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11834
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11855
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11869
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11848
BUGTRAQ	http://www.securityfocus.com/bid/101742
BUGTRAQ	http://www.securityfocus.com/bid/101725

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/101751
BUGTRAQ	http://www.securityfocus.com/bid/101753
BUGTRAQ	http://www.securityfocus.com/bid/101709
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11834
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11855
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11856
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11848
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11869
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://support.microsoft.com/en-us/help/4048957
URL	https://support.microsoft.com/en-us/help/4047206
URL	https://support.microsoft.com/en-us/help/4048955
URL	https://support.microsoft.com/en-us/help/4048954
URL	https://support.microsoft.com/en-us/help/4048959
URL	https://support.microsoft.com/en-us/help/4048952
URL	https://support.microsoft.com/en-us/help/4048958
URL	https://support.microsoft.com/en-us/help/4048953
URL	https://support.microsoft.com/en-us/help/4048956

MS17-OCT: Microsoft Internet Explorer Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-11822 - Internet Explorer Memory Corruption Vulnerability
CVE-2017-11790 - Internet Explorer Information Disclosure Vulnerability
CVE-2017-11793 - Scripting Engine Memory Corruption Vulnerability
CVE-2017-11810 - Scripting Engine Memory Corruption Vulnerability
CVE-2017-11813 - Internet Explorer Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

Solution Details

Microsoft has released a fix for this flaw in their October 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11793
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11790
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11810

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11813
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11822
BUGTRAQ	http://www.securityfocus.com/bid/101122
BUGTRAQ	http://www.securityfocus.com/bid/101077
BUGTRAQ	http://www.securityfocus.com/bid/101081
BUGTRAQ	http://www.securityfocus.com/bid/101083
BUGTRAQ	http://www.securityfocus.com/bid/101141
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11822
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11790
URL	https://support.microsoft.com/en-us/help/4042895
URL	https://support.microsoft.com/en-us/help/4041690
URL	https://support.microsoft.com/en-us/help/4040685
URL	https://support.microsoft.com/en-us/help/4041689
URL	https://support.microsoft.com/en-us/help/4041676
URL	https://support.microsoft.com/en-us/help/4041691
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11810
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11813
URL	https://support.microsoft.com/en-us/help/4041681
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11793
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://support.microsoft.com/en-us/help/4041693
URL	https://cwe.mitre.org/data/definitions/119.html

MS17-OCT: Microsoft Windows Security Update

High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2017-8689 - Win32k Elevation of Privilege Vulnerability
ADV170012 - Vulnerability in TPM could allow Security Feature Bypass
ADV170014 - Optional Windows NTLM SSO authentication changes
CVE-2017-11823 - Microsoft Windows Security Feature Bypass
CVE-2017-11786 - Skype for Business Elevation of Privilege Vulnerability
ADV170016 - Windows Server 2008 Defense in Depth
CVE-2017-8693 - Microsoft Graphics Information Disclosure Vulnerability
CVE-2017-8694 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8703 - Windows Subsystem for Linux Denial of Service Vulnerability
CVE-2017-8715 - Windows Security Feature Bypass Vulnerability
CVE-2017-8717 - Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2017-8718 - Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2017-8727 - Windows Shell Memory Corruption Vulnerability
CVE-2017-11762 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2017-11763 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2017-11765 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-11769 - TRIE Remote Code Execution Vulnerability
CVE-2017-11771 - Windows Search Remote Code Execution Vulnerability
CVE-2017-11772 - Microsoft Search Information Disclosure Vulnerability
CVE-2017-11775 - Microsoft Office SharePoint XSS Vulnerability
CVE-2017-11777 - Microsoft Office SharePoint XSS Vulnerability
CVE-2017-11779 - Windows DNSAPI Remote Code Execution Vulnerability
CVE-2017-11780 - Windows SMB Remote Code Execution Vulnerability
CVE-2017-11781 - Windows SMB Denial of Service Vulnerability
CVE-2017-11782 - Windows SMB Elevation of Privilege Vulnerability
CVE-2017-11783 - Windows Elevation of Privilege Vulnerability
CVE-2017-11784 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-11785 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-11797 - Scripting Engine Information Disclosure Vulnerability
CVE-2017-11801 - Scripting Engine Memory Corruption Vulnerability
CVE-2017-11814 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-11815 - Windows SMB Information Disclosure Vulnerability
CVE-2017-11816 - Windows GDI Information Disclosure Vulnerability
CVE-2017-11817 - Windows Information Disclosure Vulnerability
CVE-2017-11818 - Windows Storage Security Feature Bypass Vulnerability
CVE-2017-11819 - Windows Shell Remote Code Execution Vulnerability
CVE-2017-11820 - Microsoft Office SharePoint XSS Vulnerability
CVE-2017-11824 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2017-11829 - Windows Update Delivery Optimization Elevation of Privilege Vulnerability
CVE-2017-13080 - Windows Wireless WPA2/KRACK Group Key Reinstallation Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Skype for Business 2016 (64-bit)
Microsoft Lync 2013 Service Pack 1 (32-bit)
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
ChakraCore
Windows 8.1 for 32-bit systems
Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1511 for 32-bit Systems

Solution Details

Microsoft has released a fix for this flaw in their October 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11801
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11775
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11816
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8694
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8689

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11786
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11785
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11765
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-13080
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11780
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11763
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8727
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11783
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11781
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11819
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11782
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11797
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11784
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8693
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11769
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11772
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11762
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11818
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11824
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11814
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8718
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11779
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8703
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11829

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8715
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11777
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11817
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11820
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11815
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8717
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11771
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11823
BUGTRAQ	http://www.securityfocus.com/bid/101097
BUGTRAQ	http://www.securityfocus.com/bid/101105
BUGTRAQ	http://www.securityfocus.com/bid/101100
BUGTRAQ	http://www.securityfocus.com/bid/101109
BUGTRAQ	http://www.securityfocus.com/bid/101094
BUGTRAQ	http://www.securityfocus.com/bid/101142
BUGTRAQ	http://www.securityfocus.com/bid/101128
BUGTRAQ	http://www.securityfocus.com/bid/101156
BUGTRAQ	http://www.securityfocus.com/bid/101149
BUGTRAQ	http://www.securityfocus.com/bid/101111
BUGTRAQ	http://www.securityfocus.com/bid/101274
BUGTRAQ	http://www.securityfocus.com/bid/101140
BUGTRAQ	http://www.securityfocus.com/bid/101121
BUGTRAQ	http://www.securityfocus.com/bid/101143
BUGTRAQ	http://www.securityfocus.com/bid/101145
BUGTRAQ	http://www.securityfocus.com/bid/101147

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/101096
BUGTRAQ	http://www.securityfocus.com/bid/101112
BUGTRAQ	http://www.securityfocus.com/bid/101144
BUGTRAQ	http://www.securityfocus.com/bid/101116
BUGTRAQ	http://www.securityfocus.com/bid/101108
BUGTRAQ	http://www.securityfocus.com/bid/101101
BUGTRAQ	http://www.securityfocus.com/bid/101099
BUGTRAQ	http://www.securityfocus.com/bid/101093
BUGTRAQ	http://www.securityfocus.com/bid/101162
BUGTRAQ	http://www.securityfocus.com/bid/101166
BUGTRAQ	http://www.securityfocus.com/bid/101164
BUGTRAQ	http://www.securityfocus.com/bid/101213
BUGTRAQ	http://www.securityfocus.com/bid/101163
BUGTRAQ	http://www.securityfocus.com/bid/101102
BUGTRAQ	http://www.securityfocus.com/bid/101110
BUGTRAQ	http://www.securityfocus.com/bid/101155
BUGTRAQ	http://www.securityfocus.com/bid/101146
BUGTRAQ	http://www.securityfocus.com/bid/101095
BUGTRAQ	http://www.securityfocus.com/bid/101136
BUGTRAQ	http://www.securityfocus.com/bid/101161
BUGTRAQ	http://www.securityfocus.com/bid/101114
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11820
URL	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11775
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8694
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11816
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8727
URL	https://support.microsoft.com/en-us/help/4042007
URL	https://support.microsoft.com/en-us/help/4011179
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8689
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11786
URL	https://support.microsoft.com/en-us/help/4041679
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11785
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11765
URL	https://www.krackattacks.com/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-13080
URL	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2017-007.txt
URL	https://support.microsoft.com/en-us/help/4041678
URL	https://support.microsoft.com/en-us/help/4011159
URL	https://access.redhat.com/security/vulnerabilities/kracks
URL	https://support.microsoft.com/en-us/help/4042121
URL	https://support.lenovo.com/us/en/product_security/LEN-17420

Type	Reference
URL	https://support.microsoft.com/en-us/help/4011180
URL	https://w1.fi/security/2017-1/wpa-packet-number-reuse-with-replayed-messages.txt
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11763
URL	https://support.apple.com/HT208219
URL	https://support.apple.com/HT208222
URL	https://support.apple.com/HT208220
URL	https://support.apple.com/HT208325
URL	https://support.apple.com/HT208327
URL	https://support.apple.com/HT208334
URL	https://source.android.com/security/bulletin/2017-11-01
URL	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03792en_us
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-901333.pdf
URL	https://support.apple.com/HT208221
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://support.microsoft.com/en-us/help/4041687
URL	https://support.microsoft.com/en-us/help/4041690
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11781
URL	https://support.microsoft.com/en-us/help/4041689

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11819
URL	https://support.microsoft.com/en-us/help/4041676
URL	https://support.microsoft.com/en-us/help/4041691
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11782
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11797
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11784
URL	https://support.microsoft.com/en-us/help/4041693
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8693
URL	https://support.microsoft.com/en-us/help/4041681
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11769
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11783
URL	https://support.microsoft.com/en-us/help/4042895
URL	https://support.microsoft.com/en-us/help/4041944
URL	https://cert.vde.com/en-us/advisories/vde-2017-005
URL	https://support.microsoft.com/en-us/help/4011157
URL	https://cert.vde.com/en-us/advisories/vde-2017-003
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11823
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11772
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11762

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11818
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11824
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11814
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8718
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11779
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8703
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11829
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8715
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11780
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11777
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11817
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11801
URL	https://support.microsoft.com/en-us/help/4042120
URL	https://support.microsoft.com/en-us/help/4042122
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11815
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8717

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11771
URL	https://support.microsoft.com/en-us/help/4011170
URL	https://support.microsoft.com/en-us/help/4042067
URL	https://support.microsoft.com/en-us/help/4041671
URL	https://support.microsoft.com/en-us/help/4041995
URL	https://support.microsoft.com/en-us/help/4042123
URL	https://support.microsoft.com/en-us/help/4042723
URL	https://support.microsoft.com/en-us/help/4038793
URL	https://support.microsoft.com/en-us/help/4038786
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html

MS17-SEP: Microsoft Internet Explorer Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-8733 - Internet Explorer Spoofing Vulnerability
CVE-2017-8747 - Internet Explorer Memory Corruption Vulnerability
CVE-2017-8749 - Internet Explorer Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems

Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

Solution Details

Microsoft has released a fix for this flaw in their September 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8747
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8749
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8733
BUGTRAQ	http://www.securityfocus.com/bid/100737
BUGTRAQ	http://www.securityfocus.com/bid/100770
BUGTRAQ	http://www.securityfocus.com/bid/100765
URL	https://support.microsoft.com/en-us/help/4038799
URL	https://support.microsoft.com/en-us/help/4036586
URL	https://support.microsoft.com/en-us/help/4038788
URL	https://support.microsoft.com/en-us/help/4038792
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8747
URL	https://support.microsoft.com/en-us/help/4038782
URL	https://support.microsoft.com/en-us/help/4038777
URL	https://cwe.mitre.org/data/definitions/284.html

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8733
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8749
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4038783
URL	https://support.microsoft.com/en-us/help/4038781

MS17-SEP: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2017-8629 - Microsoft SharePoint XSS Vulnerability
CVE-2017-8675 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8677 - Win32k Information Disclosure Vulnerability
CVE-2017-8678 - Win32k Information Disclosure Vulnerability
CVE-2017-8679 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8680 - Win32k Information Disclosure Vulnerability
CVE-2017-8681 - Win32k Information Disclosure Vulnerability
CVE-2017-8683 - Win32k Graphics Information Disclosure Vulnerability
CVE-2017-8684 - Windows GDI+ Information Disclosure Vulnerability
CVE-2017-8685 - Windows GDI+ Information Disclosure Vulnerability
CVE-2017-8686 - Windows DHCP Server Remote Code Execution Vulnerability
CVE-2017-8687 - Win32k Information Disclosure Vulnerability
CVE-2017-8688 - Windows GDI+ Information Disclosure Vulnerability
CVE-2017-9417 - Broadcom BCM43xx Remote Code Execution Vulnerability
CVE-2017-8745 - Microsoft SharePoint Cross Site Scripting Vulnerability
CVE-2017-8758 - Microsoft Exchange Cross-Site Scripting Vulnerability
CVE-2017-0161 - NetBIOS Remote Code Execution Vulnerability
CVE-2017-8628 - Microsoft Bluetooth Driver Spoofing Vulnerability
CVE-2017-8692 - Uniscribe Remote Code Execution Vulnerability
CVE-2017-8699 - Windows Shell Remote Code Execution Vulnerability
CVE-2017-8702 - Windows Elevation of Privilege Vulnerability
CVE-2017-8704 - Hyper-V Denial of Service Vulnerability
CVE-2017-8706 - Hyper-V Information Disclosure Vulnerability
CVE-2017-8707 - Hyper-V Information Disclosure Vulnerability
CVE-2017-8708 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8709 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8710 - Windows Information Disclosure Vulnerability

CVE-2017-8711 - Hyper-V Information Disclosure Vulnerability
CVE-2017-8712 - Hyper-V Information Disclosure Vulnerability
CVE-2017-8713 - Hyper-V Information Disclosure Vulnerability
CVE-2017-8714 - Remote Desktop Virtual Host Remote Code Execution Vulnerability
CVE-2017-8716 - Windows Security Feature Bypass Vulnerability
CVE-2017-8719 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-8720 - Win32k Elevation of Privilege Vulnerability
CVE-2017-8725 - Microsoft Office Publisher Remote Code Execution
CVE-2017-8746 - Device Guard Security Feature Bypass Vulnerability
CVE-2017-11761 - Microsoft Exchange Information Disclosure Vulnerability

Affected Products:
Microsoft Publisher 2010 Service Pack 2 (32-bit editions)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Microsoft Publisher 2010 Service Pack 2 (64-bit editions)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Microsoft Publisher 2007 Service Pack 3
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Microsoft Exchange Server 2016 Cumulative Update 6
Microsoft Exchange Server 2013 Service Pack 1
Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft Exchange Server 2013 Cumulative Update 16
Microsoft Exchange Server 2013 Cumulative Update 17
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1511 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Microsoft Exchange Server 2016 Cumulative Update 5
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft SharePoint Server 2013 Service Pack 1
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their September 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8720
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8710
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8709
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8702
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0161
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8675
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8714
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8681
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8692
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8745
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8685
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8758
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8706
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8712
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11761
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8628
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8719
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8684

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8687
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8699
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8725
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9417
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8746
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8680
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8711
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8678
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8629
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8686
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8677
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8713
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8679
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8707
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8704
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8708
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8716
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8688
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8683
BUGTRAQ	http://www.securityfocus.com/bid/100787
BUGTRAQ	http://www.securityfocus.com/bid/100804
BUGTRAQ	http://www.securityfocus.com/bid/100793
BUGTRAQ	http://www.securityfocus.com/bid/100792
BUGTRAQ	http://www.securityfocus.com/bid/100785

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/100728
BUGTRAQ	http://www.securityfocus.com/bid/100752
BUGTRAQ	http://www.securityfocus.com/bid/100797
BUGTRAQ	http://www.securityfocus.com/bid/100727
BUGTRAQ	http://www.securityfocus.com/bid/100762
BUGTRAQ	http://www.securityfocus.com/bid/100753
BUGTRAQ	http://www.securityfocus.com/bid/100724
BUGTRAQ	http://www.securityfocus.com/bid/100722
BUGTRAQ	http://www.securityfocus.com/bid/100723
BUGTRAQ	http://www.securityfocus.com/bid/100789
BUGTRAQ	http://www.securityfocus.com/bid/100795
BUGTRAQ	http://www.securityfocus.com/bid/100731
BUGTRAQ	http://www.securityfocus.com/bid/100744
BUGTRAQ	http://www.securityfocus.com/bid/100803
BUGTRAQ	http://www.securityfocus.com/bid/100782
BUGTRAQ	http://www.securityfocus.com/bid/100736
BUGTRAQ	http://www.securityfocus.com/bid/100783
BUGTRAQ	http://www.securityfocus.com/bid/100758
BUGTRAQ	http://www.securityfocus.com/bid/99482
BUGTRAQ	http://www.securityfocus.com/bid/100760
BUGTRAQ	http://www.securityfocus.com/bid/100781
BUGTRAQ	http://www.securityfocus.com/bid/100794
BUGTRAQ	http://www.securityfocus.com/bid/100769
BUGTRAQ	http://www.securityfocus.com/bid/100725

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/100730
BUGTRAQ	http://www.securityfocus.com/bid/100767
BUGTRAQ	http://www.securityfocus.com/bid/100796
BUGTRAQ	http://www.securityfocus.com/bid/100720
BUGTRAQ	http://www.securityfocus.com/bid/100790
BUGTRAQ	http://www.securityfocus.com/bid/100791
BUGTRAQ	http://www.securityfocus.com/bid/100802
BUGTRAQ	http://www.securityfocus.com/bid/100756
URL	https://support.apple.com/kb/HT210121
URL	https://support.microsoft.com/en-us/help/4011113
URL	https://support.microsoft.com/en-us/help/4039325
URL	https://support.microsoft.com/en-us/help/4034786
URL	https://support.microsoft.com/en-us/help/4039038
URL	https://support.microsoft.com/en-us/help/4038874
URL	https://support.microsoft.com/en-us/help/4011117
URL	https://support.microsoft.com/en-us/help/4039266
URL	https://support.microsoft.com/en-us/help/4032201
URL	https://support.microsoft.com/en-us/help/4036108
URL	https://support.microsoft.com/en-us/help/4038779
URL	https://support.microsoft.com/en-us/help/4038786
URL	https://support.microsoft.com/en-us/help/4038793
URL	https://support.microsoft.com/en-us/help/4039384
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8720
URL	https://support.microsoft.com/en-us/help/3114428

Type	Reference
URL	https://support.microsoft.com/en-us/help/3141537
URL	https://support.microsoft.com/en-us/help/4038792
URL	https://support.microsoft.com/en-us/help/4038782
URL	https://support.microsoft.com/en-us/help/4038777
URL	https://support.microsoft.com/en-us/help/4038783
URL	https://support.microsoft.com/en-us/help/4038781
URL	https://support.microsoft.com/en-us/help/4038799
URL	https://support.microsoft.com/en-us/help/4038788
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8710
URL	https://www.youtube.com/watch?v=bIFot3a-58I
URL	https://www.vulnerability-lab.com/get_content.php?id=2094
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8709
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8702
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0161
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8675
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8714
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8681
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8692
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8745

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8685
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8680
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8758
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8706
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8712
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11761
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8628
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8719
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8684
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8687
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8699
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8725
URL	https://www.blackhat.com/us-17/briefings.html#broadpwn-remotely-compromising-android-and-ios-via-a-bug-in-broadcoms-wi-fi-chipsets
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-9417
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8746
URL	https://source.android.com/security/bulletin/2017-07-01

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8711
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8678
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8629
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8686
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8677
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8713
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8679
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8707
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8704
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8708
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8716
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8688
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8683
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/284.html

Type	Reference
URL	https://cwe.mitre.org/data/definitions/362.html
URL	https://cwe.mitre.org/data/definitions/20.html

MS18-APR: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their April 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-0987 - Scripting Engine Information Disclosure Vulnerability
CVE-2018-0988 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-0989 - Scripting Engine Information Disclosure Vulnerability
CVE-2018-0991 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-0996 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-0997 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-1000 - Scripting Engine Information Disclosure Vulnerability
CVE-2018-1001 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-1004 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2018-0870 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-0981 - Scripting Engine Information Disclosure Vulnerability
CVE-2018-1018 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-1020 - Internet Explorer Memory Corruption Vulnerability

Affected Products:
Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1511 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Internet Explorer 11 on Windows RT 8.1
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1511 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0988
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0870
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1004
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1000

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0996
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0997
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0991
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1001
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0981
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0989
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1020
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1018
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0987
BUGTRAQ	http://www.securityfocus.com/bid/103602
BUGTRAQ	http://www.securityfocus.com/bid/103603
BUGTRAQ	http://www.securityfocus.com/bid/103624
BUGTRAQ	http://www.securityfocus.com/bid/103615
BUGTRAQ	http://www.securityfocus.com/bid/103614
BUGTRAQ	http://www.securityfocus.com/bid/103623
BUGTRAQ	http://www.securityfocus.com/bid/103621
BUGTRAQ	http://www.securityfocus.com/bid/103609
BUGTRAQ	http://www.securityfocus.com/bid/103610
BUGTRAQ	http://www.securityfocus.com/bid/103618
BUGTRAQ	http://www.securityfocus.com/bid/103657
BUGTRAQ	http://www.securityfocus.com/bid/103595
BUGTRAQ	http://www.securityfocus.com/bid/103612
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0988
URL	https://support.microsoft.com/en-us/help/4093123

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1018
URL	https://support.microsoft.com/en-us/help/4093107
URL	https://support.microsoft.com/en-us/help/4093122
URL	https://support.microsoft.com/en-us/help/4093112
URL	https://support.microsoft.com/en-us/help/4093108
URL	https://support.microsoft.com/en-us/help/4092946
URL	https://support.microsoft.com/en-us/help/4093115
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0870
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1001
URL	https://support.microsoft.com/en-us/help/4093119
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1004
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://support.microsoft.com/en-us/help/4093109
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1000
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0996
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0997
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0991
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0981

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0989
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1020
URL	https://support.microsoft.com/en-us/help/4093114
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0987
URL	https://support.microsoft.com/en-us/help/4093118
URL	https://support.microsoft.com/en-us/help/4093111

MS18-APR: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-0887 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0890 - Active Directory Security Feature Bypass Vulnerability
CVE-2018-0956 - HTTP.sys Denial of Service Vulnerability
CVE-2018-0957 - Hyper-V Information Disclosure Vulnerability
CVE-2018-0960 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0963 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-0964 - Hyper-V Information Disclosure Vulnerability
CVE-2018-0966 - Device Guard Security Feature Bypass Vulnerability
CVE-2018-0967 - Windows SNMP Service Denial of Service Vulnerability
CVE-2018-0968 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0969 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0976 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2018-0970 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0971 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0972 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0973 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0974 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0975 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-1003 - Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2018-1008 - OpenType Font Driver Elevation of Privilege Vulnerability
CVE-2018-1009 - Microsoft DirectX Graphics Kernel Subsystem Elevation of Privilege Vulnerability
CVE-2018-1010 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-1012 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-1013 - Microsoft Graphics Remote Code Execution Vulnerability

CVE-2018-1015 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-1016 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-1032 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-1037 - Microsoft Visual Studio Information Disclosure Vulnerability
CVE-2018-8116 - Microsoft Graphics Component Denial of Service Vulnerability
CVE-2018-0986 - Microsoft Malware Protection Engine Remote Code Execution Vulnerability
CVE-2018-1005 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-1014 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-1034 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8117 - Microsoft Wireless Keyboard 850 Security Feature Bypass Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows Defender on Windows Server 2012
Windows 10 for 32-bit Systems
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Defender on Windows Server 2016 (Server Core installation)
Microsoft Visual Studio 2017 Version 15.7 Preview
Microsoft System Center 2012 R2 Endpoint Protection
Windows Defender on Windows Server 2012 R2 (Server Core installation)
Microsoft Visual Studio 2017 Version 15.6.6
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Defender on Windows Server 2016
Windows 8.1 for x64-based systems
Windows Defender on Windows 7 for 32-bit Systems Service Pack 1
Microsoft Visual Studio 2012 Update 5
Microsoft Visual Studio 2017
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2010 Service Pack 1
Microsoft Visual Studio 2015 Update 3
Microsoft Security Essentials
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Defender on Windows 10 Version 1511 for 32-bit Systems
Windows Defender on Windows 10 for 32-bit Systems
Windows Defender on Windows 10 for x64-based Systems
Windows Defender on Windows Server, version 1709 (Server Core Installation)
Microsoft System Center 2012 Endpoint Protection
Microsoft Forefront Endpoint Protection 2010

Windows Defender on Windows 8.1 for 32-bit systems
Microsoft Exchange Server 2016
Microsoft SharePoint Enterprise Server 2016
Microsoft Exchange Server 2013
Windows Defender on Windows 10 Version 1511 for x64-based Systems
Microsoft Wireless Keyboard 850
Windows Server 2012
Microsoft Visual Studio 2013 Update 5
Windows Defender on Windows 10 Version 1703 for x64-based Systems
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Defender on Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows Defender on Windows 10 Version 1709 for x64-based Systems
Windows Intune Endpoint Protection
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Microsoft SharePoint Server 2010 Service Pack 2
Windows Defender on Windows 10 Version 1607 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows 8.1 for x64-based systems
Windows 10 Version 1511 for x64-based Systems
Windows Defender on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1511 for 32-bit Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Defender on Windows Server 2012 R2
Microsoft System Center Endpoint Protection
Windows Defender on Windows Server 2012 (Server Core installation)
Windows Server 2016
Windows Defender on Windows 10 Version 1703 for 32-bit Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows 7 for x64-based Systems Service Pack 1
Windows Server, version 1709 (Server Core Installation)

Solution Details

Microsoft has released a fix for this flaw in their April 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1014
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1010
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0887
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1005
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1016
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8116
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1009
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0960
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1015
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0976
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1003
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1008
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0973
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0969
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1037
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1034
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0970
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1032
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1013
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0966
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1012
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0972
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0964
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0968

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8117
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0890
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0975
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0974
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0963
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0971
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0986
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0967
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0956
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0957
BUGTRAQ	http://www.securityfocus.com/bid/103645
BUGTRAQ	http://www.securityfocus.com/bid/103637
BUGTRAQ	http://www.securityfocus.com/bid/103601
BUGTRAQ	http://www.securityfocus.com/bid/103652
BUGTRAQ	http://www.securityfocus.com/bid/103632
BUGTRAQ	http://www.securityfocus.com/bid/103659
BUGTRAQ	http://www.securityfocus.com/bid/103649
BUGTRAQ	http://www.securityfocus.com/bid/103622
BUGTRAQ	http://www.securityfocus.com/bid/103705
BUGTRAQ	http://www.securityfocus.com/bid/103662
BUGTRAQ	http://www.securityfocus.com/bid/103661
BUGTRAQ	http://www.securityfocus.com/bid/103594
BUGTRAQ	http://www.securityfocus.com/bid/103646
BUGTRAQ	http://www.securityfocus.com/bid/103599

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/103643
BUGTRAQ	http://www.securityfocus.com/bid/103597
BUGTRAQ	http://www.securityfocus.com/bid/103715
BUGTRAQ	http://www.securityfocus.com/bid/103600
BUGTRAQ	http://www.securityfocus.com/bid/103663
BUGTRAQ	http://www.securityfocus.com/bid/103629
BUGTRAQ	http://www.securityfocus.com/bid/103638
BUGTRAQ	http://www.securityfocus.com/bid/103593
BUGTRAQ	http://www.securityfocus.com/bid/103658
BUGTRAQ	http://www.securityfocus.com/bid/103628
BUGTRAQ	http://www.securityfocus.com/bid/103634
BUGTRAQ	http://www.securityfocus.com/bid/103650
BUGTRAQ	http://www.securityfocus.com/bid/103651
BUGTRAQ	http://www.securityfocus.com/bid/103654
BUGTRAQ	http://www.securityfocus.com/bid/103711
BUGTRAQ	http://www.securityfocus.com/bid/103647
BUGTRAQ	http://www.securityfocus.com/bid/103655
BUGTRAQ	http://www.securityfocus.com/bid/103660
BUGTRAQ	http://www.securityfocus.com/bid/103644
BUGTRAQ	http://www.securityfocus.com/bid/103648
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0971
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1010
URL	https://support.microsoft.com/en-us/help/4091756

Type	Reference
URL	https://support.microsoft.com/en-us/help/4018336
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1005
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0967
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1016
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://support.microsoft.com/en-us/help/4087371
URL	https://support.microsoft.com/en-us/help/4089501
URL	https://support.microsoft.com/en-us/help/4018342
URL	https://support.microsoft.com/en-us/help/4011712
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0960
URL	https://support.microsoft.com/en-us/help/4089283
URL	https://support.microsoft.com/en-us/help/4093478
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1015
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1009
URL	https://support.microsoft.com/en-us/help/4093108
URL	https://support.microsoft.com/en-us/help/4093112
URL	https://support.microsoft.com/en-us/help/4093122
URL	https://support.microsoft.com/en-us/help/4093107
URL	https://support.microsoft.com/en-us/help/4093123
URL	https://support.microsoft.com/en-us/help/4093111

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0973
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0969
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1034
URL	https://support.microsoft.com/en-us/help/4093118
URL	https://support.microsoft.com/en-us/help/4093114
URL	https://support.microsoft.com/en-us/help/4093109
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1008
URL	https://support.microsoft.com/en-us/help/4093119
URL	https://support.microsoft.com/en-us/help/4093115
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0956
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0970
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0966
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0972
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1013
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1012
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0968
URL	https://support.microsoft.com/en-us/help/4093223

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0964
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0890
URL	https://support.microsoft.com/en-us/help/4093224
URL	https://support.microsoft.com/en-us/help/4093227
URL	https://cwe.mitre.org/data/definitions/310.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8117
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8116
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0975
URL	https://support.microsoft.com/en-us/help/4093257
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0974
URL	https://support.microsoft.com/en-us/help/4091346
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1003
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0963
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1037
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0887
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1014
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0986

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1032
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0957
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0976

MS18-AUG: Microsoft Internet Explorer Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-8316 - Internet Explorer Remote Code Execution Vulnerability
CVE-2018-8371 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8372 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8373 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8385 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8389 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8403 - Microsoft Browser Memory Corruption Vulnerability
CVE-2018-8351 - Microsoft Browser Information Disclosure Vulnerability
CVE-2018-8353 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8355 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8357 - Microsoft Browser Elevation of Privilege Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 for 32-bit Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1

Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

Solution Details

Microsoft has released a fix for this flaw in their August 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.3

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8355
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8385
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8371
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8403
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8351
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8372
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8353
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8357
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8316
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8389

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8373
BUGTRAQ	http://www.securityfocus.com/bid/105036
BUGTRAQ	http://www.securityfocus.com/bid/105022
BUGTRAQ	http://www.securityfocus.com/bid/105039
BUGTRAQ	http://www.securityfocus.com/bid/104978
BUGTRAQ	http://www.securityfocus.com/bid/105037
BUGTRAQ	http://www.securityfocus.com/bid/105033
BUGTRAQ	http://www.securityfocus.com/bid/105015
BUGTRAQ	http://www.securityfocus.com/bid/105038
BUGTRAQ	http://www.securityfocus.com/bid/105013
BUGTRAQ	http://www.securityfocus.com/bid/105034
BUGTRAQ	http://www.securityfocus.com/bid/105035
URL	https://support.microsoft.com/en-us/help/4343901
URL	https://support.microsoft.com/en-us/help/4343900
URL	https://support.microsoft.com/en-us/help/4343897
URL	https://support.microsoft.com/en-us/help/4343899
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8389
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8316
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8373
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8357

Type	Reference
URL	https://support.microsoft.com/en-us/help/4343205
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8353
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8372
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8351
URL	https://support.microsoft.com/en-us/help/4343892
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8403
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8371
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8385
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8355
URL	https://support.microsoft.com/en-us/help/4343887
URL	https://support.microsoft.com/en-us/help/4343909
URL	https://support.microsoft.com/en-us/help/4343885
URL	https://support.microsoft.com/en-us/help/4343898

MS18-AUG: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their August 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-8204 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability

CVE-2018-8253 - Microsoft Cortana Elevation of Privilege Vulnerability
ADV180018 - Microsoft Guidance to mitigate L1TF variant
CVE-2018-8384 - Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2018-8394 - Windows GDI Information Disclosure Vulnerability
CVE-2018-8396 - Windows GDI Information Disclosure Vulnerability
CVE-2018-8397 - GDI+ Remote Code Execution Vulnerability
CVE-2018-8398 - Windows GDI Information Disclosure Vulnerability
CVE-2018-8399 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8400 - DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8401 - DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8404 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8405 - DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8406 - DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-0952 - Diagnostic Hub Standard Collector Elevation Of Privilege Vulnerability
CVE-2018-8200 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8302 - Microsoft Exchange Memory Corruption Vulnerability
CVE-2018-8339 - Windows Installer Elevation of Privilege Vulnerability
CVE-2018-8340 - AD FS Security Feature Bypass Vulnerability
CVE-2018-8341 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8342 - Windows NDIS Elevation of Privilege Vulnerability
CVE-2018-8343 - Windows NDIS Elevation of Privilege Vulnerability
CVE-2018-8344 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2018-8345 - LNK Remote Code Execution Vulnerability
CVE-2018-8346 - LNK Remote Code Execution Vulnerability
CVE-2018-8347 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8348 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8349 - Microsoft COM for Windows Remote Code Execution Vulnerability
CVE-2018-8350 - Windows PDF Remote Code Execution Vulnerability
CVE-2018-8359 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8374 - Microsoft Exchange Server Tampering Vulnerability
CVE-2018-8414 - Windows Shell Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
ChakraCore
Windows 8.1 for 32-bit systems

Microsoft Exchange Server 2013 Cumulative Update 21
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 23
Microsoft Visual Studio 2017
Microsoft Exchange Server 2013 Cumulative Update 20
Microsoft Exchange Server 2016 Cumulative Update 10
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Server, version 1803 (Server Core Installation)
Microsoft Visual Studio 2015 Update 3
Microsoft Visual Studio 2017 Version 15.8
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Microsoft Exchange Server 2016 Cumulative Update 9
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8342
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8384
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8349
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8404
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8374
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8253
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8347
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8344

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8396
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8394
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8414
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8339
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8399
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8398
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8401
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0952
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8406
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8346
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8302
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8405
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8343
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8359
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8204
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8341
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8200
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8340
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8345
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8348
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8400
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8397
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8350
BUGTRAQ	http://www.securityfocus.com/bid/105005

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/104984
BUGTRAQ	http://www.securityfocus.com/bid/104983
BUGTRAQ	http://www.securityfocus.com/bid/105001
BUGTRAQ	http://www.securityfocus.com/bid/105030
BUGTRAQ	http://www.securityfocus.com/bid/105009
BUGTRAQ	http://www.securityfocus.com/bid/104995
BUGTRAQ	http://www.securityfocus.com/bid/104982
BUGTRAQ	http://www.securityfocus.com/bid/104987
BUGTRAQ	http://www.securityfocus.com/bid/105027
BUGTRAQ	http://www.securityfocus.com/bid/104992
BUGTRAQ	http://www.securityfocus.com/bid/104999
BUGTRAQ	http://www.securityfocus.com/bid/105029
BUGTRAQ	http://www.securityfocus.com/bid/104985
BUGTRAQ	http://www.securityfocus.com/bid/104981
BUGTRAQ	http://www.securityfocus.com/bid/104993
BUGTRAQ	http://www.securityfocus.com/bid/104988
BUGTRAQ	http://www.securityfocus.com/bid/105002
BUGTRAQ	http://www.securityfocus.com/bid/105016
BUGTRAQ	http://www.securityfocus.com/bid/105006
BUGTRAQ	http://www.securityfocus.com/bid/105012
BUGTRAQ	http://www.securityfocus.com/bid/105028
BUGTRAQ	http://www.securityfocus.com/bid/104973
BUGTRAQ	http://www.securityfocus.com/bid/105011
BUGTRAQ	http://www.securityfocus.com/bid/104990

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/105008
BUGTRAQ	http://www.securityfocus.com/bid/105007
BUGTRAQ	http://www.securityfocus.com/bid/105048
BUGTRAQ	http://www.securityfocus.com/bid/104994
BUGTRAQ	http://www.securityfocus.com/bid/104975
BUGTRAQ	http://www.securityfocus.com/bid/104998
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8404
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8374
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8253
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8347
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8344
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8396
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8394
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8414
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8339
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8399
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8398

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8401
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0952
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8406
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8346
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8302
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8405
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8343
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8359
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8204
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8341
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8200
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8340
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8345
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8348
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8400
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8397

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8350
URL	https://support.microsoft.com/en-us/help/4340937
URL	https://support.microsoft.com/en-us/help/4340731
URL	https://support.microsoft.com/en-us/help/4341832
URL	https://support.microsoft.com/en-us/help/4338380
URL	https://support.microsoft.com/en-us/help/4343674
URL	https://support.microsoft.com/en-us/help/4344104
URL	https://support.microsoft.com/en-us/help/4343896
URL	https://support.microsoft.com/en-us/help/4340733
URL	https://support.microsoft.com/en-us/help/4343888
URL	https://support.microsoft.com/en-us/help/4340939
URL	https://support.microsoft.com/en-us/help/4343899
URL	https://support.microsoft.com/en-us/help/4343897
URL	https://support.microsoft.com/en-us/help/4343900
URL	https://support.microsoft.com/en-us/help/4343901
URL	https://support.microsoft.com/en-us/help/4343898
URL	https://support.microsoft.com/en-us/help/4343885
URL	https://support.microsoft.com/en-us/help/4343909
URL	https://support.microsoft.com/en-us/help/4343887
URL	https://support.microsoft.com/en-us/help/4343892
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180018
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8342

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8384
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8349
URL	https://cwe.mitre.org/data/definitions/94.html
URL	https://cwe.mitre.org/data/definitions/502.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/254.html

MS18-DEC: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their December 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-8619 - Internet Explorer Remote Code Execution Vulnerability
CVE-2018-8625 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2018-8631 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-8643 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8653 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems

Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8619
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8643
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8631
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8625
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8653
BUGTRAQ	http://www.securityfocus.com/bid/106118
BUGTRAQ	http://www.securityfocus.com/bid/106117
BUGTRAQ	http://www.securityfocus.com/bid/106255
BUGTRAQ	http://www.securityfocus.com/bid/106119
BUGTRAQ	http://www.securityfocus.com/bid/106122
URL	https://support.microsoft.com/en-us/help/4471321
URL	https://support.microsoft.com/help/4483234
URL	https://support.microsoft.com/help/4483229
URL	https://support.microsoft.com/en-us/help/4471329

Type	Reference
URL	https://nvd.nist.gov/vuln/detail/CVE-2018-8653
URL	https://support.microsoft.com/help/4483187
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8619
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8625
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8653
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8643
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8631
URL	https://support.microsoft.com/en-us/help/4471330
URL	https://support.microsoft.com/en-us/help/4471325
URL	https://support.microsoft.com/en-us/help/4471318
URL	https://support.microsoft.com/en-us/help/4471324
URL	https://support.microsoft.com/en-us/help/4471332
URL	https://support.microsoft.com/en-us/help/4471327
URL	https://support.microsoft.com/help/4483235
URL	https://support.microsoft.com/help/4483232
URL	https://support.microsoft.com/en-us/help/4471320
URL	https://support.microsoft.com/help/4483228
URL	https://support.microsoft.com/help/4483230
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4471323
URL	https://support.microsoft.com/en-us/help/4470199

MS18-DEC: Microsoft Windows Security Update

High

Solution Details

Microsoft has released a fix for this flaw in their December 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-8477 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8514 - Remote Procedure Call runtime Information Disclosure Vulnerability
CVE-2018-8595 - Windows GDI Information Disclosure Vulnerability
CVE-2018-8596 - Windows GDI Information Disclosure Vulnerability
CVE-2018-8604 - Microsoft Exchange Server Tampering Vulnerability
CVE-2018-8580 - Microsoft SharePoint Information Disclosure Vulnerability
CVE-2018-8599 - Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2018-8611 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8612 - Connected User Experiences and Telemetry Service Denial of Service Vulnerability
CVE-2018-8621 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8622 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8626 - Windows DNS Server Heap Overflow Vulnerability
CVE-2018-8634 - Microsoft Text-To-Speech Remote Code Execution Vulnerability
CVE-2018-8635 - Microsoft SharePoint Server Elevation of Privilege Vulnerability
CVE-2018-8637 - Win32k Information Disclosure Vulnerability
CVE-2018-8638 - DirectX Information Disclosure Vulnerability
CVE-2018-8639 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8641 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8649 - Windows Denial of Service Vulnerability
CVE-2018-8651 - Microsoft Dynamics NAV Cross Site Scripting Vulnerability
CVE-2018-8652 - Windows Azure Pack Cross Site Scripting Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Microsoft Exchange Server 2016 Cumulative Update 11
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Microsoft SharePoint Server 2010 Service Pack 2
Windows 8.1 for 32-bit systems
Windows Azure Pack Rollup 13.1
Microsoft Visual Studio 2017
Microsoft Exchange Server 2016 Cumulative Update 10
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1803 for 32-bit Systems
Microsoft Dynamics NAV 2016
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Dynamics NAV 2017
Windows Server, version 1803 (Server Core Installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Microsoft Visual Studio 2015 Update 3
Microsoft SharePoint Foundation 2010 Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8652
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8596

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8634
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8580
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8621
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8651
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8514
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8612
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8626
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8595
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8611
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8635
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8638
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8477
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8641
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8639
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8622
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8649
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8599
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8604
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8637
BUGTRAQ	http://www.securityfocus.com/bid/106077
BUGTRAQ	http://www.securityfocus.com/bid/106088
BUGTRAQ	http://www.securityfocus.com/bid/106093
BUGTRAQ	http://www.securityfocus.com/bid/106090
BUGTRAQ	http://www.securityfocus.com/bid/106081

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/106082
BUGTRAQ	http://www.securityfocus.com/bid/106083
BUGTRAQ	http://www.securityfocus.com/bid/106079
BUGTRAQ	http://www.securityfocus.com/bid/106085
BUGTRAQ	http://www.securityfocus.com/bid/106086
BUGTRAQ	http://www.securityfocus.com/bid/106094
BUGTRAQ	http://www.securityfocus.com/bid/106155
BUGTRAQ	http://www.securityfocus.com/bid/106078
BUGTRAQ	http://www.securityfocus.com/bid/106096
BUGTRAQ	http://www.securityfocus.com/bid/106087
BUGTRAQ	http://www.securityfocus.com/bid/106076
BUGTRAQ	http://www.securityfocus.com/bid/106121
BUGTRAQ	http://www.securityfocus.com/bid/106089
BUGTRAQ	http://www.securityfocus.com/bid/106091
BUGTRAQ	http://www.securityfocus.com/bid/106103
BUGTRAQ	http://www.securityfocus.com/bid/106095
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4471323
URL	https://support.microsoft.com/en-us/help/4471320
URL	https://support.microsoft.com/en-us/help/4471324
URL	https://support.microsoft.com/en-us/help/4471318
URL	https://support.microsoft.com/en-us/help/4471325
URL	https://support.microsoft.com/en-us/help/4471330

Type	Reference
URL	https://support.microsoft.com/en-us/help/4461541
URL	https://support.microsoft.com/en-us/help/4461549
URL	https://support.microsoft.com/en-us/help/4471326
URL	https://support.microsoft.com/en-us/help/4479232
URL	https://support.microsoft.com/en-us/help/4469516
URL	https://support.microsoft.com/en-us/help/4471319
URL	https://support.microsoft.com/en-us/help/4461558
URL	https://support.microsoft.com/en-us/help/4461465
URL	https://support.microsoft.com/en-us/help/4471322
URL	https://support.microsoft.com/en-us/help/4471328
URL	https://support.microsoft.com/en-us/help/4468741
URL	https://support.microsoft.com/en-us/help/4461580
URL	https://support.microsoft.com/en-us/help/4479233
URL	https://support.microsoft.com/en-us/help/4480788
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8652
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8596
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8634
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8580
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8621
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8651
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8514

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8612
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8626
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8595
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8611
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8635
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8638
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8477
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8641
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8639
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8622
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8649
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8599
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8604
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8637
URL	https://support.microsoft.com/en-us/help/4471332
URL	https://support.microsoft.com/en-us/help/4471327
URL	https://support.microsoft.com/en-us/help/4471321

Type	Reference
URL	https://support.microsoft.com/en-us/help/4471329
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/20.html

MS18-FEB: Microsoft Internet Explorer Security Update

High

Solution Details

Microsoft has released a fix for this flaw in their February 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

PLEASE NOTE: If this patch is not being offered by Windows Update please verify that the following registry key exists and your antivirus software is up to date. Otherwise Windows Update will return no available patches while the system remains vulnerable.

Key="HKEY_LOCAL_MACHINE"Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompa

Value Name="cadca5fe-87d3-4b96-b7fb-a231484277cc"
Type="REG_DWORD”
Data="0x00000000”

Microsoft has issued this guidance to all antivirus vendors, that they must set this registry key to signal to Windows Update that they are compatible with the latest 2018 updates.

If this registry key does not exist, the system is still vulnerable but Windows Update may not offer to the patch to the affected system. Please contact your antivirus vendor, or install Windows Defender on the affected system to resolve this condition and allow the system to continue receiving normal updates.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-0840 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-0866 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems

Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge on Windows 10 for 32-bit Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0840
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0866
BUGTRAQ	http://www.securityfocus.com/bid/102886
BUGTRAQ	http://www.securityfocus.com/bid/103032
URL	https://support.microsoft.com/en-us/help/4074596
URL	https://support.microsoft.com/en-us/help/4074594

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0866
URL	https://support.microsoft.com/en-us/help/4074588
URL	https://support.microsoft.com/en-us/help/4074593
URL	https://support.microsoft.com/en-us/help/4074592
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0840
URL	https://support.microsoft.com/en-us/help/4074736
URL	https://support.microsoft.com/en-us/help/4074598
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4074591
URL	https://support.microsoft.com/en-us/help/4074590

MS18-FEB: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their February 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

PLEASE NOTE: If this patch is not being offered by Windows Update please verify that the following registry key exists and your antivirus software is up to date. Otherwise Windows Update will return no available patches while the system remains vulnerable.

Key="HKEY_LOCAL_MACHINE"Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompa

Value Name="cadca5fe-87d3-4b96-b7fb-a231484277cc"
Type="REG_DWORD”
Data="0x00000000”

Microsoft has issued this guidance to all antivirus vendors, that they must set this registry key to signal to Windows Update that they are compatible with the latest 2018 updates. Please contact your antivirus vendor, or install Windows Defender on the affected system to resolve this condition and allow the system to continue receiving normal updates.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-0810 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0827 - Windows Security Feature Bypass Vulnerability
CVE-2018-0828 - Windows Elevation of Privilege Vulnerability
CVE-2018-0829 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0830 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0831 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-0832 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0833 - Windows Denial of Service Vulnerability
CVE-2018-0842 - Windows Remote Code Execution Vulnerability
CVE-2018-0843 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0847 - Windows Scripting Engine Memory Corruption Vulnerability
CVE-2018-0855 - Windows EOT Font Engine Information Disclosure Vulnerability
CVE-2018-0858 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-0869 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0742 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-0755 - Windows EOT Font Engine Information Disclosure Vulnerability
CVE-2018-0756 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-0809 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-0820 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-0821 - Windows AppContainer Elevation Of Privilege Vulnerability
CVE-2018-0822 - Windows NTFS Global Reparse Point Elevation of Privilege Vulnerability
CVE-2018-0823 - Named Pipe File System Elevation of Privilege Vulnerability
CVE-2018-0825 - StructuredQuery Remote Code Execution Vulnerability
CVE-2018-0826 - Windows Storage Services Elevation of Privilege Vulnerability
CVE-2018-0844 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2018-0846 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2018-0864 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0757 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0760 - Windows EOT Font Engine Information Disclosure Vulnerability
CVE-2018-0761 - Windows EOT Font Engine Information Disclosure Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
ChakraCore

Windows 8.1 for 32-bit systems
Microsoft Project Server 2013 Service Pack 1
Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1511 for 32-bit Systems
Windows Server 2016 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0826
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0832
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0844
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0864
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0843
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0833
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0831
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0761
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0823
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0742
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0847

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0822
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0810
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0827
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0825
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0846
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0829
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0757
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0755
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0842
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0760
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0820
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0855
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0821
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0828
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0756
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0869
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0809
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0858
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0830
BUGTRAQ	http://www.securityfocus.com/bid/102951
BUGTRAQ	http://www.securityfocus.com/bid/102962
BUGTRAQ	http://www.securityfocus.com/bid/102929
BUGTRAQ	http://www.securityfocus.com/bid/102923
BUGTRAQ	http://www.securityfocus.com/bid/102944

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/102949
BUGTRAQ	http://www.securityfocus.com/bid/102933
BUGTRAQ	http://www.securityfocus.com/bid/102924
BUGTRAQ	http://www.securityfocus.com/bid/102943
BUGTRAQ	http://www.securityfocus.com/bid/102952
BUGTRAQ	http://www.securityfocus.com/bid/102919
BUGTRAQ	http://www.securityfocus.com/bid/102937
BUGTRAQ	http://www.securityfocus.com/bid/102861
BUGTRAQ	http://www.securityfocus.com/bid/102942
BUGTRAQ	http://www.securityfocus.com/bid/102938
BUGTRAQ	http://www.securityfocus.com/bid/102927
BUGTRAQ	http://www.securityfocus.com/bid/102931
BUGTRAQ	http://www.securityfocus.com/bid/102948
BUGTRAQ	http://www.securityfocus.com/bid/102947
BUGTRAQ	http://www.securityfocus.com/bid/102934
BUGTRAQ	http://www.securityfocus.com/bid/102946
BUGTRAQ	http://www.securityfocus.com/bid/102953
BUGTRAQ	http://www.securityfocus.com/bid/102945
BUGTRAQ	http://www.securityfocus.com/bid/102936
BUGTRAQ	http://www.securityfocus.com/bid/102939
BUGTRAQ	http://www.securityfocus.com/bid/102935
BUGTRAQ	http://www.securityfocus.com/bid/102941
BUGTRAQ	http://www.securityfocus.com/bid/102963
BUGTRAQ	http://www.securityfocus.com/bid/102865

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/102920
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0847
URL	https://support.microsoft.com/en-us/help/4074598
URL	https://support.microsoft.com/en-us/help/4074591
URL	https://support.microsoft.com/en-us/help/4074593
URL	https://support.microsoft.com/en-us/help/4074590
URL	https://support.microsoft.com/en-us/help/4074596
URL	https://support.microsoft.com/en-us/help/4074594
URL	https://support.microsoft.com/en-us/help/4074588
URL	https://support.microsoft.com/en-us/help/4074592
URL	https://support.microsoft.com/en-us/help/4074836
URL	https://support.microsoft.com/en-us/help/4034044
URL	https://support.microsoft.com/en-us/help/4073079
URL	https://support.microsoft.com/en-us/help/4074587
URL	https://support.microsoft.com/en-us/help/4011680
URL	https://support.microsoft.com/en-us/help/4058165
URL	https://support.microsoft.com/en-us/help/4073080
URL	https://support.microsoft.com/en-us/help/4011701
URL	https://support.microsoft.com/en-us/help/4074603
URL	https://support.microsoft.com/en-us/help/4074589
URL	https://support.microsoft.com/en-us/help/4074597
URL	https://support.microsoft.com/en-us/help/4074851
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0843

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0864
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0844
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0832
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0826
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0830
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0858
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0809
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0833
URL	https://github.com/KINGSABRI/CVE-in-Ruby/tree/master/CVE-2018-0833
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0831
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0761
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0823
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0742
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0822
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0810
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0827

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0825
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0846
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0829
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0757
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0755
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0842
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0760
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0820
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0855
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0821
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0828
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0756
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0869
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/476.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference

MS18-JAN: Microsoft Internet Explorer Security Update (MELTDOWN) High

Solution Details

Microsoft has released a fix for this flaw in their January 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

PLEASE NOTE: If this patch is not being offered by Windows Update please verify that the following registry key exists and your antivirus software is up to date. Otherwise Windows Update will return no available patches while the system remains vulnerable.

Key="HKEY_LOCAL_MACHINE"Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompa

Value Name="cadca5fe-87d3-4b96-b7fb-a231484277cc"
Type="REG_DWORD”
Data="0x00000000”

Microsoft has issued this guidance to all antivirus vendors, that they must set this registry key to signal to Windows Update that they are compatible with the latest 2018 updates. Please contact your antivirus vendor, or install Windows Defender on the affected system to resolve this condition and allow the system to continue receiving normal updates.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-5754 - Meltdown CPU Flaw
CVE-2018-0762 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-0772 - Scripting Engine Memory Corruption Vulnerability

Meltdown (CVE-2017-5754) can be leveraged by a malicious program running on the local system to read memory from other processes, including the operating system. Additionally, it may be possible for a malicious program running inside a virtual machine to read memory from the host operating system. This can result in the disclosure of sensitive information which may lead to further compromise.

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems

Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0772
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5754
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0762
BUGTRAQ	http://www.securityfocus.com/bid/102408
BUGTRAQ	http://www.securityfocus.com/bid/106128
BUGTRAQ	http://www.securityfocus.com/bid/102409
URL	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2018-001.txt
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4611
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0772
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://meltdownattack.com/

Type	Reference
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4609
URL	https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html
URL	https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html
URL	https://developer.arm.com/support/security-update
URL	https://support.microsoft.com/en-us/help/4056888
URL	https://www.codeaurora.org/security-bulletin/2018/07/02/july-2018-code-aurora-security-bulletin
URL	https://support.f5.com/csp/article/K91229003
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03871en_us
URL	https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/
URL	https://support.lenovo.com/us/en/solutions/LEN-18282
URL	https://support.citrix.com/article/CTX234679
URL	https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/
URL	https://aws.amazon.com/de/security/security-bulletins/AWS-2018-013/
URL	https://source.android.com/security/bulletin/2018-04-01
URL	https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-18-0001
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0762
URL	https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability
URL	https://security.netapp.com/advisory/ntap-20180104-0001/
URL	https://support.citrix.com/article/CTX231399
URL	https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-hpesbhf03805en_us

Type	Reference
URL	https://access.redhat.com/security/vulnerabilities/speculativeexecution
URL	https://support.microsoft.com/en-us/help/4056568
URL	https://help.ecostruxureit.com/display/public/UADCO8x/StruxureWare+Data+Center+Operation+Software+Vulnerability+Fixes
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4613
URL	https://cert.vde.com/en-us/advisories/vde-2018-002
URL	https://www.synology.com/support/security/Synology_SA_18_01
URL	https://cert.vde.com/en-us/advisories/vde-2018-003
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4614
URL	https://01.org/security/advisories/intel-oss-10003
URL	https://support.microsoft.com/en-us/help/4056890
URL	https://support.microsoft.com/en-us/help/4056891
URL	https://support.microsoft.com/en-us/help/4056892
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
URL	http://xenbits.xen.org/xsa/advisory-254.html
URL	https://support.microsoft.com/en-us/help/4056893

MS18-JUL: Microsoft Internet Explorer Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-0949 - Internet Explorer Security Feature Bypass Vulnerability
CVE-2018-8242 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8287 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8288 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8291 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8296 - Scripting Engine Memory Corruption Vulnerability

Affected Products:

Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 for 32-bit Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

Solution Details

Microsoft has released a fix for this flaw in their July 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8296

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0949
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8242
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8288
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8291
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8287
BUGTRAQ	http://www.securityfocus.com/bid/104638
BUGTRAQ	http://www.securityfocus.com/bid/104622
BUGTRAQ	http://www.securityfocus.com/bid/104620
BUGTRAQ	http://www.securityfocus.com/bid/104636
BUGTRAQ	http://www.securityfocus.com/bid/104637
BUGTRAQ	http://www.securityfocus.com/bid/104634
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8296
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0949
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8242
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8288
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8291
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8287
URL	https://support.microsoft.com/en-us/help/4338829
URL	https://support.microsoft.com/en-us/help/4338826

Type	Reference
URL	https://support.microsoft.com/en-us/help/4338814
URL	https://support.microsoft.com/en-us/help/4338830
URL	https://support.microsoft.com/en-us/help/4338819
URL	https://support.microsoft.com/en-us/help/4339093
URL	https://support.microsoft.com/en-us/help/4338815
URL	https://support.microsoft.com/en-us/help/4338818
URL	https://support.microsoft.com/en-us/help/4338825

MS18-JUL: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-8172 - Visual Studio Remote Code Execution Vulnerability
CVE-2018-8206 - Windows FTP Server Denial of Service Vulnerability
CVE-2018-8222 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8232 - Microsoft Macro Assembler Tampering Vulnerability
CVE-2018-8282 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8283 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8298 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8313 - Windows Elevation of Privilege Vulnerability
CVE-2018-8319 - MSR JavaScript Cryptography Library Security Feature Bypass Vulnerability
CVE-2018-8323 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8326 - Open Source Customization for Active Directory Federation Services XSS Vulnerability
CVE-2018-8327 - PowerShell Editor Services Remote Code Execution Vulnerability
CVE-2018-8238 - Skype for Business and Lync Security Feature Bypass Vulnerability
CVE-2018-8299 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8300 - Microsoft SharePoint Remote Code Execution Vulnerability
CVE-2018-8304 - Windows DNSAPI Denial of Service Vulnerability
CVE-2018-8305 - Windows Mail Client Information Disclosure Vulnerability
CVE-2018-8306 - Microsoft Wireless Display Adapter Command Injection Vulnerability
CVE-2018-8307 - WordPad Security Feature Bypass Vulnerability
CVE-2018-8308 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8309 - Windows Denial of Service Vulnerability
CVE-2018-8311 - Remote Code Execution Vulnerability in Skype For Business and Lync
CVE-2018-8314 - Windows Elevation of Privilege Vulnerability

Affected Products:

Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2017 Version 15.7.5
Windows 10 for 32-bit Systems
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Microsoft Visual Studio 2013 Update 5
Windows 7 for x64-based Systems Service Pack 1
Skype for Business 2016 (64-bit)
Microsoft Lync 2013 Service Pack 1 (32-bit)
Windows 10 Version 1803 for x64-based Systems
Mail, Calendar, and People in Windows 8.1 App Store
Microsoft Wireless Display Adapter V2 Software Version 2.0.8350
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Microsoft Visual Studio 2017 Version 15.8 Preview
Microsoft Lync 2013 Service Pack 1 (64-bit)
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Web Customizations for Active Directory Federation Services
Windows Server 2012 R2
ChakraCore
Windows 8.1 for 32-bit systems
Microsoft Visual Studio 2012 Update 5
Microsoft Visual Studio 2017
Microsoft Wireless Display Adapter V2 Software Version 2.0.8365
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server, version 1803 (Server Core Installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Microsoft Visual Studio 2010 Service Pack 1
Microsoft Visual Studio 2015 Update 3
Windows 10 Version 1703 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Microsoft SharePoint Foundation 2013 Service Pack 1
Skype for Business 2016 (32-bit)
Expression Blend 4 Service Pack 3
PowerShell Extension for Visual Studio Code

Windows Server 2016
Microsoft Research JavaScript Cryptography Library
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
PowerShell Editor Services
Microsoft Wireless Display Adapter V2 Software Version 2.0.8372
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their July 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8238
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8309
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8222
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8283
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8299
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8300
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8304
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8323
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8326
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8298
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8306
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8232
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8308
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8319
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8172

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8307
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8206
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8313
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8305
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8282
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8314
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8327
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8311
BUGTRAQ	http://www.securityfocus.com/bid/104621
BUGTRAQ	http://www.securityfocus.com/bid/104640
BUGTRAQ	http://www.securityfocus.com/bid/104655
BUGTRAQ	http://www.securityfocus.com/bid/104616
BUGTRAQ	http://www.securityfocus.com/bid/104631
BUGTRAQ	http://www.securityfocus.com/bid/104629
BUGTRAQ	http://www.securityfocus.com/bid/104670
BUGTRAQ	http://www.securityfocus.com/bid/104619
BUGTRAQ	http://www.securityfocus.com/bid/104618
BUGTRAQ	http://www.securityfocus.com/bid/104668
BUGTRAQ	http://www.securityfocus.com/bid/104652
BUGTRAQ	http://www.securityfocus.com/bid/104649
BUGTRAQ	http://www.securityfocus.com/bid/104624
BUGTRAQ	http://www.securityfocus.com/bid/104614
BUGTRAQ	http://www.securityfocus.com/bid/104617
BUGTRAQ	http://www.securityfocus.com/bid/104611

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/104648
BUGTRAQ	http://www.securityfocus.com/bid/104635
BUGTRAQ	http://www.securityfocus.com/bid/104633
BUGTRAQ	http://www.securityfocus.com/bid/104610
BUGTRAQ	http://www.securityfocus.com/bid/104639
BUGTRAQ	http://www.securityfocus.com/bid/104656
URL	https://support.microsoft.com/en-us/help/4339854
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8304
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8300
URL	https://support.microsoft.com/en-us/help/4340583
URL	https://support.microsoft.com/en-us/help/4342193
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/682.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.microsoft.com/en-us/help/4022228
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8309
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8222
URL	https://support.microsoft.com/en-us/help/4336919
URL	https://support.microsoft.com/en-us/help/4336986
URL	https://support.microsoft.com/en-us/help/4295656
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8323
URL	https://support.microsoft.com/en-us/help/4338829

Type	Reference
URL	https://support.microsoft.com/en-us/help/4338826
URL	https://support.microsoft.com/en-us/help/4338814
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/77.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4338830
URL	https://support.microsoft.com/en-us/help/4338819
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8238
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8283
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8299
URL	https://support.microsoft.com/en-us/help/4338820
URL	https://support.microsoft.com/en-us/help/4291391
URL	https://support.microsoft.com/en-us/help/4338815
URL	https://support.microsoft.com/en-us/help/4338824
URL	https://support.microsoft.com/en-us/help/4338818
URL	https://support.microsoft.com/en-us/help/4338825
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8311
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8327
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8314

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8282
URL	https://support.microsoft.com/en-us/help/4338823
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8305
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8313
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8206
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8307
URL	https://support.microsoft.com/en-us/help/4339503
URL	https://support.microsoft.com/en-us/help/4336946
URL	https://support.microsoft.com/en-us/help/4022243
URL	https://support.microsoft.com/en-us/help/4022225
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8172
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8319
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8308
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8232
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8306
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8298
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8326
URL	https://support.microsoft.com/en-us/help/4022235

Type	Reference
URL	https://support.microsoft.com/en-us/help/4293756
URL	https://support.microsoft.com/en-us/help/4336999
URL	https://support.microsoft.com/en-us/help/4339291
URL	https://support.microsoft.com/en-us/help/4022221

MS18-JUN: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their June 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-0978 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-8113 - Internet Explorer Security Feature Bypass Vulnerability
CVE-2018-8249 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-8267 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8113
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8249
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8267
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0978
BUGTRAQ	http://www.securityfocus.com/bid/104364
BUGTRAQ	http://www.securityfocus.com/bid/104365
BUGTRAQ	http://www.securityfocus.com/bid/104363
BUGTRAQ	http://www.securityfocus.com/bid/104404
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8113
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8267
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8249
URL	https://support.microsoft.com/en-us/help/4284880
URL	https://support.microsoft.com/en-us/help/4284860
URL	https://support.microsoft.com/en-us/help/4284815
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4284835
URL	https://support.microsoft.com/en-us/help/4284855
URL	https://support.microsoft.com/en-us/help/4284819
URL	https://support.microsoft.com/en-us/help/4284826

Type	Reference
URL	https://support.microsoft.com/en-us/help/4230450
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0978
URL	https://support.microsoft.com/en-us/help/4284874

MS18-JUN: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-8175 - WEBDAV Denial of Service Vulnerability
CVE-2018-8140 - Cortana Elevation of Privilege Vulnerability
CVE-2018-8201 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8205 - Windows Denial of Service Vulnerability
CVE-2018-8207 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8208 - Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2018-8209 - Windows Wireless Network Profile Information Disclosure Vulnerability
CVE-2018-8210 - Windows Remote Code Execution Vulnerability
CVE-2018-8211 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8212 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8213 - Windows Remote Code Execution Vulnerability
CVE-2018-8214 - Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2018-8215 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8216 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8217 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8218 - Windows Hyper-V Denial of Service Vulnerability
CVE-2018-8219 - Hypervisor Code Integrity Elevation of Privilege Vulnerability
CVE-2018-8221 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8224 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8225 - Windows DNSAPI Remote Code Execution Vulnerability
CVE-2018-8226 - HTTP.sys Denial of Service Vulnerability
CVE-2018-8231 - HTTP Protocol Stack Remote Code Execution Vulnerability
CVE-2018-8233 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8239 - Windows GDI Information Disclosure Vulnerability
CVE-2018-8243 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8245 - Microsoft Office Elevation of Privilege Vulnerability
CVE-2018-8252 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8254 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0982 - Windows Elevation of Privilege Vulnerability
CVE-2018-1036 - NTFS Elevation of Privilege Vulnerability

CVE-2018-1040 - Windows Code Integrity Module Denial of Service Vulnerability
CVE-2018-8121 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8169 - HIDParser Elevation of Privilege Vulnerability
CVE-2018-8251 - Media Foundation Memory Corruption Vulnerability

Affected Products:
Microsoft Publisher 2010 Service Pack 2 (32-bit editions)
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Microsoft Publisher 2010 Service Pack 2 (64-bit editions)
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
ChakraCore
Windows 8.1 for 32-bit systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Server, version 1803 (Server Core Installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft Project Server 2010 Service Pack 2
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their June 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8213
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8219
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8233
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8175
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8121
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8209
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8252
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8205
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8221
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8251
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8217
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8218
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8208
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0982
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8140
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8211
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8216
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8239
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8226
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8243
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1040

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8224
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1036
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8225
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8201
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8212
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8254
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8245
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8210
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8215
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8169
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8214
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8207
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8231
BUGTRAQ	http://www.securityfocus.com/bid/104395
BUGTRAQ	http://www.securityfocus.com/bid/104407
BUGTRAQ	http://www.securityfocus.com/bid/104356
BUGTRAQ	http://www.securityfocus.com/bid/104328
BUGTRAQ	http://www.securityfocus.com/bid/104331
BUGTRAQ	http://www.securityfocus.com/bid/104381
BUGTRAQ	http://www.securityfocus.com/bid/104403
BUGTRAQ	http://www.securityfocus.com/bid/104361
BUGTRAQ	http://www.securityfocus.com/bid/104401
BUGTRAQ	http://www.securityfocus.com/bid/104334
BUGTRAQ	http://www.securityfocus.com/bid/104326

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/104354
BUGTRAQ	http://www.securityfocus.com/bid/104382
BUGTRAQ	http://www.securityfocus.com/bid/104402
BUGTRAQ	http://www.securityfocus.com/bid/104337
BUGTRAQ	http://www.securityfocus.com/bid/104338
BUGTRAQ	http://www.securityfocus.com/bid/104317
BUGTRAQ	http://www.securityfocus.com/bid/104393
BUGTRAQ	http://www.securityfocus.com/bid/104380
BUGTRAQ	http://www.securityfocus.com/bid/104359
BUGTRAQ	http://www.securityfocus.com/bid/104353
BUGTRAQ	http://www.securityfocus.com/bid/104406
BUGTRAQ	http://www.securityfocus.com/bid/104373
BUGTRAQ	http://www.securityfocus.com/bid/104383
BUGTRAQ	http://www.securityfocus.com/bid/104398
BUGTRAQ	http://www.securityfocus.com/bid/104392
BUGTRAQ	http://www.securityfocus.com/bid/104389
BUGTRAQ	http://www.securityfocus.com/bid/104360
BUGTRAQ	http://www.securityfocus.com/bid/104379
BUGTRAQ	http://www.securityfocus.com/bid/104333
BUGTRAQ	http://www.securityfocus.com/bid/104391
BUGTRAQ	http://www.securityfocus.com/bid/104394
BUGTRAQ	http://www.securityfocus.com/bid/104405
BUGTRAQ	http://www.securityfocus.com/bid/104325
URL	https://cwe.mitre.org/data/definitions/200.html

Type	Reference
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4284867
URL	https://support.microsoft.com/en-us/help/4230467
URL	https://support.microsoft.com/en-us/help/4284860
URL	https://support.microsoft.com/en-us/help/4284855
URL	https://support.microsoft.com/en-us/help/4284874
URL	https://support.microsoft.com/en-us/help/4284815
URL	https://support.microsoft.com/en-us/help/4284880
URL	https://support.microsoft.com/en-us/help/4284826
URL	https://support.microsoft.com/en-us/help/4284819
URL	https://support.microsoft.com/en-us/help/4284835
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1036
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8225
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8210
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8169
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8212
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8201
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8224
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8243
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8226

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8239
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8216
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8211
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8140
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8205
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0982
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8218
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8217
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8221
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8252
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8209
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8121
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8175

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8219
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8213
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8231
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8215
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8251
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8233
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://support.microsoft.com/en-us/help/4022190
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8208
URL	https://support.microsoft.com/en-us/help/4234459
URL	https://support.microsoft.com/en-us/help/4284846
URL	https://support.microsoft.com/en-us/help/4284878
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1040
URL	https://support.microsoft.com/en-us/help/4022210
URL	https://support.microsoft.com/en-us/help/4294413
URL	https://support.microsoft.com/en-us/help/4011186
URL	https://support.microsoft.com/en-us/help/4022173
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8207
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8245

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8214
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8254

MS18-MAR: Microsoft Internet Explorer Security Update

High

Solution Details

Microsoft has released a fix for this flaw in their March 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-0889 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-0891 - Scripting Engine Information Disclosure Vulnerability
CVE-2018-0927 - Microsoft Browser Information Disclosure Vulnerability
CVE-2018-0929 - Internet Explorer Information Disclosure Vulnerability
CVE-2018-0932 - Microsoft Browser Information Disclosure Vulnerability
CVE-2018-0935 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-0942 - Internet Explorer Elevation of Privilege Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge on Windows 10 for 32-bit Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012

Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Edge on Windows 10 Version 1511 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0932
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0935
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0942
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0889
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0929
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0927
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0891
BUGTRAQ	http://www.securityfocus.com/bid/103298
BUGTRAQ	http://www.securityfocus.com/bid/103307
BUGTRAQ	http://www.securityfocus.com/bid/103295
BUGTRAQ	http://www.securityfocus.com/bid/103312
BUGTRAQ	http://www.securityfocus.com/bid/103299
BUGTRAQ	http://www.securityfocus.com/bid/103310

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/103309
URL	https://support.microsoft.com/en-us/help/4088776
URL	https://support.microsoft.com/en-us/help/4088875
URL	https://support.microsoft.com/en-us/help/4088787
URL	https://support.microsoft.com/en-us/help/4088786
URL	https://support.microsoft.com/en-us/help/4088782
URL	https://support.microsoft.com/en-us/help/4088876
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0932
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0942
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0935
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0889
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0929
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0927
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0891
URL	https://support.microsoft.com/en-us/help/4088779
URL	https://support.microsoft.com/en-us/help/4089187
URL	https://support.microsoft.com/en-us/help/4088877

MS18-MAR: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-0811 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0816 - Windows GDI Elevation of Privilege Vulnerability
CVE-2018-0817 - Windows GDI Elevation of Privilege Vulnerability
CVE-2018-0868 - Windows Installer Elevation of Privilege Vulnerability
CVE-2018-0884 - Windows Security Feature Bypass Vulnerability
CVE-2018-0885 - Windows Hyper-V Denial of Service Vulnerability
CVE-2018-0886 - CredSSP Remote Code Execution Vulnerability
CVE-2018-0888 - Hyper-V Information Disclosure Vulnerability
CVE-2018-0894 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0895 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0896 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0897 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0898 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0899 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0900 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0901 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0902 - CNG Security Feature Bypass Vulnerability
CVE-2018-0924 - Microsoft Exchange Information Disclosure Vulnerability
CVE-2018-0926 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0940 - Microsoft Exchange Elevation of Privilege Vulnerability
CVE-2018-0941 - Microsoft Exchange Information Disclosure Vulnerability
CVE-2018-0947 - Microsoft Sharepoint Elevation of Privilege Vulnerability
CVE-2018-0977 - Win32k Elevation of Privilege Vulnerability
CVE-2018-0983 - Windows Storage Services Elevation of Privilege Vulnerability
CVE-2018-0813 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0814 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0815 - Windows GDI Elevation of Privilege Vulnerability
CVE-2018-0877 - Windows Desktop Bridge VFS Elevation of Privilege Vulnerability
CVE-2018-0878 - Windows Remote Assistance Information Disclosure Vulnerability
CVE-2018-0880 - Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2018-0881 - Microsoft Video Control Elevation of Privilege Vulnerability
CVE-2018-0882 - Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2018-0883 - Windows Shell Remote Code Execution Vulnerability
CVE-2018-0904 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-0909 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0910 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0911 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0912 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0913 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0914 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0915 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0916 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0917 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0921 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-0923 - Microsoft SharePoint Elevation of Privilege Vulnerability

CVE-2018-0925 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-0944 - Microsoft SharePoint Elevation of Privilege Vulnerability

Affected Products:
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 20
Microsoft Exchange Server 2013 Cumulative Update 19
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Exchange Server 2013 Cumulative Update 18
Microsoft Exchange Server 2016 Cumulative Update 7
Windows 10 for 32-bit Systems
Microsoft Exchange Server 2016 Cumulative Update 8
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
ChakraCore
Windows 8.1 for 32-bit systems
Microsoft Project Server 2013 Service Pack 1
Microsoft Exchange Server 2013 Service Pack 1
Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1511 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft SharePoint Foundation 2013 Service Pack 1
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

Solution Details

Microsoft has released a fix for this flaw in their March 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0983
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0912
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0896
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0895
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0914
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0923
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0917
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0911
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0888
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0894
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0817
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0916
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0868
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0885
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0947
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0902
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0898
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0915
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0901
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0904

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0878
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0877
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0926
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0944
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0925
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0881
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0909
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0884
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0813
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0882
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0815
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0924
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0940
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0883
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0897
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0900
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0814
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0941
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0921
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0913
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0910
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0811
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0886
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0977

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0899
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0880
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0816
BUGTRAQ	http://www.securityfocus.com/bid/103381
BUGTRAQ	http://www.securityfocus.com/bid/103285
BUGTRAQ	http://www.securityfocus.com/bid/103240
BUGTRAQ	http://www.securityfocus.com/bid/103238
BUGTRAQ	http://www.securityfocus.com/bid/103291
BUGTRAQ	http://www.securityfocus.com/bid/103308
BUGTRAQ	http://www.securityfocus.com/bid/103281
BUGTRAQ	http://www.securityfocus.com/bid/103231
BUGTRAQ	http://www.securityfocus.com/bid/103296
BUGTRAQ	http://www.securityfocus.com/bid/103262
BUGTRAQ	http://www.securityfocus.com/bid/103249
BUGTRAQ	http://www.securityfocus.com/bid/103294
BUGTRAQ	http://www.securityfocus.com/bid/103236
BUGTRAQ	http://www.securityfocus.com/bid/103261
BUGTRAQ	http://www.securityfocus.com/bid/103306
BUGTRAQ	http://www.securityfocus.com/bid/103266
BUGTRAQ	http://www.securityfocus.com/bid/103242
BUGTRAQ	http://www.securityfocus.com/bid/103247
BUGTRAQ	http://www.securityfocus.com/bid/103293
BUGTRAQ	http://www.securityfocus.com/bid/103245
BUGTRAQ	http://www.securityfocus.com/bid/103246

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/103230
BUGTRAQ	http://www.securityfocus.com/bid/103227
BUGTRAQ	http://www.securityfocus.com/bid/103304
BUGTRAQ	http://www.securityfocus.com/bid/103287
BUGTRAQ	http://www.securityfocus.com/bid/103256
BUGTRAQ	http://www.securityfocus.com/bid/103279
BUGTRAQ	http://www.securityfocus.com/bid/103248
BUGTRAQ	http://www.securityfocus.com/bid/103260
BUGTRAQ	http://www.securityfocus.com/bid/103257
BUGTRAQ	http://www.securityfocus.com/bid/103234
BUGTRAQ	http://www.securityfocus.com/bid/103320
BUGTRAQ	http://www.securityfocus.com/bid/103323
BUGTRAQ	http://www.securityfocus.com/bid/103244
BUGTRAQ	http://www.securityfocus.com/bid/103250
BUGTRAQ	http://www.securityfocus.com/bid/103259
BUGTRAQ	http://www.securityfocus.com/bid/103241
BUGTRAQ	http://www.securityfocus.com/bid/103251
BUGTRAQ	http://www.securityfocus.com/bid/103318
BUGTRAQ	http://www.securityfocus.com/bid/103302
BUGTRAQ	http://www.securityfocus.com/bid/103290
BUGTRAQ	http://www.securityfocus.com/bid/103280
BUGTRAQ	http://www.securityfocus.com/bid/103265
BUGTRAQ	http://www.securityfocus.com/bid/103380
BUGTRAQ	http://www.securityfocus.com/bid/103243

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/103239
BUGTRAQ	http://www.securityfocus.com/bid/103232
URL	https://support.microsoft.com/en-us/help/4073011
URL	https://support.microsoft.com/en-us/help/4056564
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://github.com/preempt/credssp
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0983
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0912
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0896
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0895
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0914
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0923
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0911
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0917
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0894
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0888
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0817

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0916
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0868
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0885
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0947
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0902
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0898
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0915
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0901
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0904
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0878
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0877
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0926
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0944
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0925
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0881
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0909

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0816
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0884
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0882
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0815
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0924
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0940
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0813
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0900
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0883
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0897
URL	https://blog.preempt.com/security-advisory-credssp
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0814
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0941
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0921
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0913
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0910

Type	Reference
URL	https://ics-cert.us-cert.gov/advisories/ICSA-18-198-03
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0886
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0977
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0899
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0880
URL	https://support.microsoft.com/en-us/help/4089229
URL	https://support.microsoft.com/en-us/help/4018298
URL	https://support.microsoft.com/en-us/help/4073537
URL	https://support.microsoft.com/en-us/help/4088879
URL	https://support.microsoft.com/en-us/help/4073392
URL	https://support.microsoft.com/en-us/help/4089344
URL	https://support.microsoft.com/en-us/help/4087398
URL	https://support.microsoft.com/en-us/help/4089453
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0811
URL	https://cwe.mitre.org/data/definitions/611.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://support.microsoft.com/en-us/help/4089175
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.microsoft.com/en-us/help/4088779
URL	https://support.microsoft.com/en-us/help/4088877
URL	https://support.microsoft.com/en-us/help/4088776

Type	Reference
URL	https://support.microsoft.com/en-us/help/4088875
URL	https://support.microsoft.com/en-us/help/4088787
URL	https://support.microsoft.com/en-us/help/4088786
URL	https://support.microsoft.com/en-us/help/4088782
URL	https://support.microsoft.com/en-us/help/4088876
URL	https://support.microsoft.com/en-us/help/4018304
URL	https://support.microsoft.com/en-us/help/4088878
URL	https://support.microsoft.com/en-us/help/4018293
URL	https://support.microsoft.com/en-us/help/4018305
URL	https://support.microsoft.com/en-us/help/4088880
URL	https://support.microsoft.com/en-us/help/4088827

MS18-MAY: Microsoft Internet Explorer Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-8122 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8126 - Internet Explorer Security Feature Bypass Vulnerability
CVE-2018-8145 - Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2018-0954 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-0955 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-1022 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-1025 - Microsoft Browser Information Disclosure Vulnerability
CVE-2018-8114 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8178 - Microsoft Browser Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows 10 for x64-based Systems

Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

Solution Details

Microsoft has released a fix for this flaw in their May 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8114
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0955
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0954
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8126
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8122

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1025
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8178
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1022
BUGTRAQ	http://www.securityfocus.com/bid/103994
BUGTRAQ	http://www.securityfocus.com/bid/103978
BUGTRAQ	http://www.securityfocus.com/bid/103995
BUGTRAQ	http://www.securityfocus.com/bid/103991
BUGTRAQ	http://www.securityfocus.com/bid/103986
BUGTRAQ	http://www.securityfocus.com/bid/103984
BUGTRAQ	http://www.securityfocus.com/bid/103997
BUGTRAQ	http://www.securityfocus.com/bid/104076
BUGTRAQ	http://www.securityfocus.com/bid/103993
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0954
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1022
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8145
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8126
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8122
URL	https://support.microsoft.com/en-us/help/4103768
URL	https://support.microsoft.com/en-us/help/4103721

Type	Reference
URL	https://support.microsoft.com/en-us/help/4103730
URL	https://support.microsoft.com/en-us/help/4103727
URL	https://support.microsoft.com/en-us/help/4103716
URL	https://support.microsoft.com/en-us/help/4103718
URL	https://support.microsoft.com/en-us/help/4103731
URL	https://support.microsoft.com/en-us/help/4103723
URL	https://support.microsoft.com/en-us/help/4103725
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1025
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8178
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0955
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8114

MS18-MAY: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-0854 - Windows Security Feature Bypass Vulnerability
CVE-2018-0958 - Windows Security Feature Bypass Vulnerability
CVE-2018-0959 - Hyper-V Remote Code Execution Vulnerability
CVE-2018-0961 - Hyper-V vSMB Remote Code Execution Vulnerability
CVE-2018-8119 - Azure IoT SDK Spoofing Vulnerability
CVE-2018-8124 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8127 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8129 - Windows Security Feature Bypass Vulnerability
CVE-2018-8132 - Windows Security Feature Bypass Vulnerability
CVE-2018-8134 - Windows Elevation of Privilege Vulnerability
CVE-2018-8136 - Windows Remote Code Execution Vulnerability
CVE-2018-8897 - Windows Kernel Elevation of Privilege Vulnerability

CVE-2018-8151 - Microsoft Exchange Memory Corruption Vulnerability
CVE-2018-8152 - Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2018-8154 - Microsoft Exchange Memory Corruption Vulnerability
CVE-2018-8155 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8156 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8164 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8165 - DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8166 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8167 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2018-8168 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8173 - Microsoft InfoPath Remote Code Execution Vulnerability
CVE-2018-8177 - Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2018-0824 - Microsoft COM for Windows Remote Code Execution Vulnerability
CVE-2018-8115 - Windows Host Compute Service Shim Remote Code Execution Vulnerability
CVE-2018-8120 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8141 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8149 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8153 - Microsoft Exchange Spoofing Vulnerability
CVE-2018-8159 - Microsoft Exchange Elevation of Privilege Vulnerability
CVE-2018-8170 - Windows Image Elevation of Privilege Vulnerability
CVE-2018-8174 - Windows VBScript Engine Remote Code Execution Vulnerability

Affected Products:
Microsoft Exchange Server 2013 Cumulative Update 19
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Host Compute Service Shim
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 21
Microsoft Exchange Server 2016 Cumulative Update 8
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Microsoft Infopath 2013 Service Pack 1 (32-bit edition)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Microsoft Infopath 2013 Service Pack 1 (64-bit edition)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
ChakraCore
Microsoft SharePoint Server 2010 Service Pack 2
Windows 8.1 for 32-bit systems
Microsoft Project Server 2013 Service Pack 1

C# SDK for Azure IoT
Microsoft Exchange Server 2013 Service Pack 1
Microsoft Exchange Server 2013 Cumulative Update 20
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Java SDK for Azure IoT
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Server, version 1803 (Server Core Installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Microsoft SharePoint Foundation 2013 Service Pack 1
Microsoft Project Server 2010 Service Pack 2
Microsoft Exchange Server 2016 Cumulative Update 9
C SDK for Azure IoT
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

Solution Details

Microsoft has released a fix for this flaw in their May 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.6

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8177
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8165
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0959
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8152
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8151
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8159

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8134
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8153
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8166
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8124
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8132
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0958
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8897
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0854
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8164
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8141
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8170
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8119
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8127
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0961
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8136
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8120
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8167
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8173
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8168
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8174
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8155
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8154
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8149
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8115

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8129
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0824
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8156
BUGTRAQ	http://www.securityfocus.com/bid/104066
BUGTRAQ	http://www.securityfocus.com/bid/104033
BUGTRAQ	http://www.securityfocus.com/bid/104078
BUGTRAQ	http://www.securityfocus.com/bid/104068
BUGTRAQ	http://www.securityfocus.com/bid/104070
BUGTRAQ	http://www.securityfocus.com/bid/104040
BUGTRAQ	http://www.securityfocus.com/bid/104032
BUGTRAQ	http://www.securityfocus.com/bid/104044
BUGTRAQ	http://www.securityfocus.com/bid/104034
BUGTRAQ	http://www.securityfocus.com/bid/104042
BUGTRAQ	http://www.securityfocus.com/bid/104043
BUGTRAQ	http://www.securityfocus.com/bid/104056
BUGTRAQ	http://www.securityfocus.com/bid/104041
BUGTRAQ	http://www.securityfocus.com/bid/104045
BUGTRAQ	http://www.securityfocus.com/bid/104061
BUGTRAQ	http://www.securityfocus.com/bid/104090
BUGTRAQ	http://www.securityfocus.com/bid/104037
BUGTRAQ	http://www.securityfocus.com/bid/104048
BUGTRAQ	http://www.securityfocus.com/bid/104036
BUGTRAQ	http://www.securityfocus.com/bid/104063
BUGTRAQ	http://www.securityfocus.com/bid/104069

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/104067
BUGTRAQ	http://www.securityfocus.com/bid/104054
BUGTRAQ	http://www.securityfocus.com/bid/104047
BUGTRAQ	http://www.securityfocus.com/bid/104031
BUGTRAQ	http://www.securityfocus.com/bid/104062
BUGTRAQ	http://www.securityfocus.com/bid/104065
BUGTRAQ	http://www.securityfocus.com/bid/104030
BUGTRAQ	http://www.securityfocus.com/bid/103998
BUGTRAQ	http://www.securityfocus.com/bid/104029
BUGTRAQ	http://www.securityfocus.com/bid/104064
BUGTRAQ	http://www.securityfocus.com/bid/104071
BUGTRAQ	http://www.securityfocus.com/bid/104038
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8149
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8132
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8115
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1567074
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8897
URL	https://support.apple.com/HT208742
URL	https://svnweb.freebsd.org/base?view=revision&revision=333368
URL	https://www.freebsd.org/security/advisories/FreeBSD-SA-18:06.debugreg.asc
URL	https://xenbits.xen.org/xsa/advisory-260.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8164

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8141
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8170
URL	https://github.com/torvalds/linux/commit/d8ba61ba58c88d5207c1ba2f7d9a2280e7d03be9
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8119
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8127
URL	http://openwall.com/lists/oss-security/2018/05/08/4
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0961
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8136
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8177
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8165
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8152
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8159
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8134
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8153
URL	https://support.citrix.com/article/CTX234679
URL	https://cwe.mitre.org/data/definitions/295.html
URL	https://cwe.mitre.org/data/definitions/502.html

Type	Reference
URL	http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=d8ba61ba58c88d5207c1ba2f7d9a2280e7d03be9
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8151
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8124
URL	https://github.com/can1357/CVE-2018-8897/
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://openwall.com/lists/oss-security/2018/05/08/1
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8154
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8156
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8120
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8167
URL	https://support.microsoft.com/en-us/help/4022145
URL	https://support.microsoft.com/en-us/help/4103715
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8173
URL	https://support.microsoft.com/en-us/help/4018381
URL	https://support.microsoft.com/en-us/help/4134651
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8168
URL	https://support.microsoft.com/en-us/help/4092041
URL	https://support.microsoft.com/en-us/help/4103726

Type	Reference
URL	https://support.microsoft.com/en-us/help/4101477
URL	https://support.microsoft.com/en-us/help/4018398
URL	https://support.microsoft.com/en-us/help/4018390
URL	https://support.microsoft.com/en-us/help/3162075
URL	https://support.microsoft.com/en-us/help/4022130
URL	https://support.microsoft.com/en-us/help/4091243
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8155
URL	https://support.microsoft.com/en-us/help/3114889
URL	https://support.microsoft.com/en-us/help/4103712
URL	https://support.microsoft.com/en-us/help/4131188
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0959
URL	https://support.microsoft.com/en-us/help/4130944
URL	https://support.microsoft.com/en-us/help/4094079
URL	https://support.microsoft.com/en-us/help/4103721
URL	https://support.microsoft.com/en-us/help/4103730
URL	https://support.microsoft.com/en-us/help/4103718
URL	https://security.netapp.com/advisory/ntap-20180927-0002/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8166
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8129
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0824
URL	https://support.microsoft.com/en-us/help/4103716
URL	https://support.microsoft.com/en-us/help/4103731

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8174
URL	https://tools.cisco.com/security/center/viewAlert.x?alertId=57754&vs_f=Alert%20RSS&vs_cat=Security%20Intelligence&vs_type=RSS&vs_p=Microsoft%20Azure%20IoT%20SDK%20AMQP%20Transport%20Library%20Spoofing%20Vulnerability&vs_k=1
URL	https://support.microsoft.com/en-us/help/4103723
URL	https://support.microsoft.com/en-us/help/4103725
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://support.microsoft.com/en-us/help/4103727
URL	https://blog.0patch.com/2018/05/a-single-instruction-micropatch-for.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0854
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0958
URL	https://patchwork.kernel.org/patch/10386677/
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://www.synology.com/support/security/Synology_SA_18_21
URL	https://www.triplefault.io/2018/05/spurious-db-exceptions-with-pop-ss.html

MS18-NOV: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-8256 - Microsoft PowerShell Remote Code Execution Vulnerability
CVE-2018-8407 - MSRPC Information Disclosure Vulnerability
CVE-2018-8415 - Microsoft PowerShell Tampering Vulnerability
CVE-2018-8417 - Microsoft JScript Security Feature Bypass Vulnerability
CVE-2018-8454 - Windows Audio Service Information Disclosure Vulnerability
CVE-2018-8471 - Microsoft RemoteFX Virtual GPU miniport driver Elevation of Privilege Vulnerability
CVE-2018-8476 - Windows Deployment Services TFTP Server Remote Code Execution Vulnerability
CVE-2018-8485 - DirectX Elevation of Privilege Vulnerability

CVE-2018-8553 - Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2018-8554 - DirectX Elevation of Privilege Vulnerability
CVE-2018-8561 - DirectX Elevation of Privilege Vulnerability
CVE-2018-8562 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8563 - DirectX Information Disclosure Vulnerability
CVE-2018-8565 - Win32k Information Disclosure Vulnerability
CVE-2018-8566 - BitLocker Security Feature Bypass Vulnerability
CVE-2018-8572 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8581 - Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2018-8600 - Azure App Service Cross-site Scripting Vulnerability
CVE-2018-8589 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2018-8592 - Windows Elevation Of Privilege Vulnerability
CVE-2018-8605 - Microsoft Dynamics 365 (on-premises) version 8 Cross Site Scripting Vulnerability
CVE-2018-8606 - Microsoft Dynamics 365 (on-premises) version 8 Cross Site Scripting Vulnerability
CVE-2018-8607 - Microsoft Dynamics 365 (on-premises) version 8 Cross Site Scripting Vulnerability
CVE-2018-8608 - Microsoft Dynamics 365 (on-premises) version 8 Cross Site Scripting Vulnerability
CVE-2018-8609 - Microsoft Dynamics 365 (on-premises) version 8 Remote Code Execution Vulnerability
CVE-2018-8408 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8450 - Windows Search Remote Code Execution Vulnerability
CVE-2018-8544 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2018-8547 - Active Directory Federation Services XSS Vulnerability
CVE-2018-8549 - Windows Security Feature Bypass Vulnerability
CVE-2018-8550 - Windows COM Elevation of Privilege Vulnerability
CVE-2018-8568 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8578 - Microsoft SharePoint Information Disclosure Vulnerability
CVE-2018-8584 - Windows ALPC Elevation of Privilege Vulnerability
ADV180028 - Guidance for configuring BitLocker to enforce software encryption
CVE-2018-8602 - Team Foundation Server Cross-site Scripting Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Dynamics 365 (on-premises) version 8
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Microsoft Exchange Server 2016
Azure App Service on Azure Stack
Microsoft Exchange Server 2013
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
PowerShell Core 6.1

Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Microsoft Exchange Server 2019
Team Foundation Server 2018 Update 3
Team Foundation Server 2017 Update 3.1
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1803 for 32-bit Systems
PowerShell Core 6.0
Microsoft Exchange Server 2010
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Team Foundation Server 2018 Update 3.1
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Team Foundation Server 2018 Update 1.1
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Microsoft SharePoint Foundation 2013 Service Pack 1
Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft SharePoint Server 2019
Windows Server, version 1709 (Server Core Installation)

Solution Details

Microsoft has released a fix for this flaw in their November 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8605
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8554
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8415
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8544
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8256
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8589
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8407
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8584
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8578
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8602
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8549
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8550
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8608
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8485
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8600
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8568
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8454
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8553
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8565
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8476
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8561
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8566
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8562
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8408

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8606
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8581
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8450
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8417
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8572
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8592
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8609
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8547
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8607
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8471
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8563
BUGTRAQ	http://www.securityfocus.com/bid/105794
BUGTRAQ	http://www.securityfocus.com/bid/105831
BUGTRAQ	http://www.securityfocus.com/bid/105778
BUGTRAQ	http://www.securityfocus.com/bid/105800
BUGTRAQ	http://www.securityfocus.com/bid/105891
BUGTRAQ	http://www.securityfocus.com/bid/105801
BUGTRAQ	http://www.securityfocus.com/bid/105894
BUGTRAQ	http://www.securityfocus.com/bid/105809
BUGTRAQ	http://www.securityfocus.com/bid/105797
BUGTRAQ	http://www.securityfocus.com/bid/105837
BUGTRAQ	http://www.securityfocus.com/bid/105890
BUGTRAQ	http://www.securityfocus.com/bid/105790
BUGTRAQ	http://www.securityfocus.com/bid/105806

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/105813
BUGTRAQ	http://www.securityfocus.com/bid/105774
BUGTRAQ	http://www.securityfocus.com/bid/105791
BUGTRAQ	http://www.securityfocus.com/bid/105777
BUGTRAQ	http://www.securityfocus.com/bid/105799
BUGTRAQ	http://www.securityfocus.com/bid/105829
BUGTRAQ	http://www.securityfocus.com/bid/105893
BUGTRAQ	http://www.securityfocus.com/bid/105770
BUGTRAQ	http://www.securityfocus.com/bid/105892
BUGTRAQ	http://www.securityfocus.com/bid/105805
BUGTRAQ	http://www.securityfocus.com/bid/105803
BUGTRAQ	http://www.securityfocus.com/bid/105895
BUGTRAQ	http://www.securityfocus.com/bid/105832
BUGTRAQ	http://www.securityfocus.com/bid/105796
BUGTRAQ	http://www.securityfocus.com/bid/105787
BUGTRAQ	http://www.securityfocus.com/bid/105811
BUGTRAQ	http://www.securityfocus.com/bid/105889
BUGTRAQ	http://www.securityfocus.com/bid/105789
BUGTRAQ	http://www.securityfocus.com/bid/105781
BUGTRAQ	http://www.securityfocus.com/bid/105792
BUGTRAQ	http://www.securityfocus.com/bid/105808
BUGTRAQ	http://www.securityfocus.com/bid/105795
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/20.html

Type	Reference
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/416.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://cwe.mitre.org/data/definitions/94.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://support.microsoft.com/en-us/help/4467706
URL	https://support.microsoft.com/en-us/help/4467691
URL	https://support.microsoft.com/en-us/help/4467701
URL	https://support.microsoft.com/en-us/help/4467107
URL	https://support.microsoft.com/en-us/help/4467680
URL	https://support.microsoft.com/en-us/help/4467686
URL	https://support.microsoft.com/en-us/help/4467697
URL	https://support.microsoft.com/en-us/help/4467696
URL	https://support.microsoft.com/en-us/help/4467702
URL	https://support.microsoft.com/en-us/help/4467708
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180028
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8605
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8554
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8415

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8544
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8256
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8589
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8407
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8584
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8578
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8602
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8549
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8550
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8608
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8485
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8600
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8568
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8454
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8553
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8565

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8476
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8561
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8566
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8562
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8408
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8606
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8581
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8450
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8417
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8572
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8592
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8609
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8547
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8607
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8471
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8563

Type	Reference
URL	https://support.microsoft.com/en-us/help/4461483
URL	https://support.microsoft.com/en-us/help/4465663
URL	https://support.microsoft.com/en-us/help/3173424
URL	https://support.microsoft.com/en-us/help/4461511
URL	https://support.microsoft.com/en-us/help/4465659
URL	https://support.microsoft.com/en-us/help/4467700
URL	https://support.microsoft.com/en-us/help/4465661
URL	https://support.microsoft.com/en-us/help/4093430
URL	https://support.microsoft.com/en-us/help/3177467
URL	https://support.microsoft.com/en-us/help/4467678
URL	https://support.microsoft.com/en-us/help/3173426
URL	https://support.microsoft.com/en-us/help/4467675
URL	https://support.microsoft.com/en-us/help/3020369
URL	https://support.microsoft.com/en-us/help/4465660
URL	https://support.microsoft.com/en-us/help/4461513
URL	https://support.microsoft.com/en-us/help/4467703
URL	https://support.microsoft.com/en-us/help/4461501
URL	https://support.microsoft.com/en-us/help/4467106
URL	https://support.microsoft.com/en-us/help/4465664

MS18-OCT: Microsoft Internet Explorer Security Update — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their October 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-8460 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-8491 - Internet Explorer Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8491
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8460
BUGTRAQ	http://www.securityfocus.com/bid/105454
BUGTRAQ	http://www.securityfocus.com/bid/105449
URL	https://support.microsoft.com/en-us/help/4464330

Type	Reference
URL	https://support.microsoft.com/en-us/help/4462937
URL	https://support.microsoft.com/en-us/help/4462926
URL	https://support.microsoft.com/en-us/help/4462918
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4462923
URL	https://support.microsoft.com/en-us/help/4462949
URL	https://support.microsoft.com/en-us/help/4462917
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8491
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8460
URL	https://support.microsoft.com/en-us/help/4462919
URL	https://support.microsoft.com/en-us/help/4462922

MS18-OCT: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-8320 - Windows DNS Security Feature Bypass Vulnerability
CVE-2018-8329 - Linux On Windows Elevation Of Privilege Vulnerability
CVE-2018-8330 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8333 - Microsoft Filter Manager Elevation Of Privilege Vulnerability
CVE-2018-8411 - NTFS Elevation of Privilege Vulnerability
CVE-2018-8413 - Windows Theme API Remote Code Execution Vulnerability
CVE-2018-8453 - Win32k Elevation of Privilege Vulnerability
CVE-2018-8480 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8481 - Windows Media Player Information Disclosure Vulnerability
CVE-2018-8482 - Windows Media Player Information Disclosure Vulnerability
CVE-2018-8484 - DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8486 - DirectX Information Disclosure Vulnerability
CVE-2018-8488 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8506 - Microsoft Windows Codecs Library Information Disclosure Vulnerability
CVE-2018-8518 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8423 - Microsoft JET Database Engine Remote Code Execution Vulnerability

CVE-2018-8265 - Microsoft Exchange Remote Code Execution Vulnerability
CVE-2018-8448 - Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2018-8472 - Windows GDI Information Disclosure Vulnerability
CVE-2018-8489 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2018-8490 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2018-8492 - Device Guard Code Integrity Policy Security Feature Bypass Vulnerability
CVE-2018-8493 - Windows TCP/IP Information Disclosure Vulnerability
CVE-2018-8494 - MS XML Remote Code Execution Vulnerability
CVE-2018-8495 - Windows Shell Remote Code Execution Vulnerability
CVE-2018-8497 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8498 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8500 - Scripting Engine Memory Corruption Vulnerability
CVE-2010-3190 - MFC Insecure Library Loading Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Microsoft Exchange Server 2016
Microsoft Exchange Server 2013
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
ChakraCore
Windows 8.1 for 32-bit systems
Microsoft Exchange Server 2013 Cumulative Update 21
Microsoft Exchange Server 2016 Cumulative Update 10
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Exchange Server 2010 Service Pack 3
Windows Server, version 1803 (Server Core Installation)
Windows 7 for 32-bit Systems Service Pack 1

Windows RT 8.1
Windows 10 Version 1703 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

Solution Details

Microsoft has released a fix for this flaw in their October 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8498
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8472
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-3190
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8492
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8423
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8488
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8482
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8329
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8518
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8490
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8330
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8320
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8265

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8484
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8486
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8448
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8480
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8500
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8489
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8497
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8481
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8413
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8493
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8453
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8494
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8333
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8506
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8495
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8411
BUGTRAQ	http://www.securityfocus.com/bid/42811
BUGTRAQ	http://www.securityfocus.com/bid/105508
BUGTRAQ	http://www.securityfocus.com/bid/105461
BUGTRAQ	http://www.securityfocus.com/bid/105507
BUGTRAQ	http://www.securityfocus.com/bid/105457
BUGTRAQ	http://www.securityfocus.com/bid/105463
BUGTRAQ	http://www.securityfocus.com/bid/105493
BUGTRAQ	http://www.securityfocus.com/bid/105492

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/105501
BUGTRAQ	http://www.securityfocus.com/bid/105500
BUGTRAQ	http://www.securityfocus.com/bid/105491
BUGTRAQ	http://www.securityfocus.com/bid/105503
BUGTRAQ	http://www.securityfocus.com/bid/105477
BUGTRAQ	http://www.securityfocus.com/bid/105480
BUGTRAQ	http://www.securityfocus.com/bid/105496
BUGTRAQ	http://www.securityfocus.com/bid/105505
BUGTRAQ	http://www.securityfocus.com/bid/105494
BUGTRAQ	http://www.securityfocus.com/bid/105478
BUGTRAQ	http://www.securityfocus.com/bid/105488
BUGTRAQ	http://www.securityfocus.com/bid/105455
BUGTRAQ	http://www.securityfocus.com/bid/105469
BUGTRAQ	http://www.securityfocus.com/bid/105479
BUGTRAQ	http://www.securityfocus.com/bid/105452
BUGTRAQ	http://www.securityfocus.com/bid/105448
BUGTRAQ	http://www.securityfocus.com/bid/105456
BUGTRAQ	http://www.securityfocus.com/bid/105467
BUGTRAQ	http://www.securityfocus.com/bid/105466
BUGTRAQ	http://www.securityfocus.com/bid/105495
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8413
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8453
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8494

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8333
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8506
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8495
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8411
URL	https://support.microsoft.com/en-us/help/4461450
URL	https://support.microsoft.com/en-us/help/4461447
URL	https://support.microsoft.com/en-us/help/4462931
URL	https://support.microsoft.com/en-us/help/4463097
URL	https://support.microsoft.com/en-us/help/4462929
URL	https://support.microsoft.com/en-us/help/4462941
URL	https://support.microsoft.com/en-us/help/4462915
URL	https://support.microsoft.com/en-us/help/4463104
URL	https://support.microsoft.com/en-us/help/4459266
URL	https://support.microsoft.com/en-us/help/2565063
URL	http://packetstormsecurity.com/files/153669/Microsoft-Windows-NtUserSetWindowFNID-Win32k-User-Callback.html
URL	https://support.apple.com/HT205221
URL	https://support.microsoft.com/en-us/help/4462919
URL	https://support.microsoft.com/en-us/help/4462922
URL	https://cwe.mitre.org/data/definitions/611.html
URL	https://leucosite.com/Microsoft-Edge-RCE/
URL	https://blog.0patch.com/2018/10/patching-re-patching-and-meta-patching.html

Type	Reference
URL	https://blog.0patch.com/2018/09/outrunning-attackers-on-jet-database.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2011/ms11-025
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://securelist.com/cve-2018-8453-used-in-targeted-attack
URL	https://support.microsoft.com/en-us/help/4462917
URL	https://support.microsoft.com/en-us/help/4462923
URL	https://support.microsoft.com/en-us/help/4462918
URL	https://support.microsoft.com/en-us/help/4462926
URL	https://support.microsoft.com/en-us/help/4462937
URL	https://support.microsoft.com/en-us/help/4464330
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8498
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8472
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2010-3190
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8492
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8423
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8488

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8482
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8329
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8518
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8490
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8330
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8320
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8265
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8484
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8486
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8448
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8480
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8500
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8489
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8497
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8481
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8493

MS18-SEP: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their September 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-8315 - Microsoft Scripting Engine Information Disclosure Vulnerability
CVE-2018-8461 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-8447 - Internet Explorer Memory Corruption Vulnerability
CVE-2018-8452 - Scripting Engine Information Disclosure Vulnerability
CVE-2018-8457 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8470 - Internet Explorer Security Feature Bypass Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems

Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8447
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8452
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8315
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8461
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8457
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8470
BUGTRAQ	http://www.securityfocus.com/bid/105252
BUGTRAQ	http://www.securityfocus.com/bid/105257
BUGTRAQ	http://www.securityfocus.com/bid/105267
BUGTRAQ	http://www.securityfocus.com/bid/105207
BUGTRAQ	http://www.securityfocus.com/bid/105258
BUGTRAQ	http://www.securityfocus.com/bid/105251
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8447
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8452
URL	https://support.microsoft.com/en-us/help/4457144
URL	https://support.microsoft.com/en-us/help/4457129
URL	https://support.microsoft.com/en-us/help/4457135

Type	Reference
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://support.microsoft.com/en-us/help/4457131
URL	https://support.microsoft.com/en-us/help/4457132
URL	https://support.microsoft.com/en-us/help/4457128
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8470
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8457
URL	https://support.microsoft.com/en-us/help/4457426
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8461
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4457142
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8315
URL	https://support.microsoft.com/en-us/help/4458010
URL	https://support.microsoft.com/en-us/help/4457138

MS18-SEP: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their September 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2018-0965 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2018-8269 - OData Denial of Service Vulnerability
CVE-2018-8271 - Windows Information Disclosure Vulnerability
CVE-2018-8335 - Windows SMB Denial of Service Vulnerability

CVE-2018-8336 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8410 - Windows Registry Elevation of Privilege Vulnerability
CVE-2018-8419 - Windows Kernel Information Disclosure Vulnerability
ADV180022 - Windows Denial of Service Vulnerability
CVE-2018-8420 - MS XML Remote Code Execution Vulnerability
CVE-2018-8422 - Windows GDI Information Disclosure Vulnerability
CVE-2018-8424 - Windows GDI Information Disclosure Vulnerability
CVE-2018-8433 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2018-8462 - DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2018-8475 - Windows Remote Code Execution Vulnerability
CVE-2018-8337 - Windows Subsystem for Linux Security Feature Bypass Vulnerability
CVE-2018-8391 - Scripting Engine Memory Corruption Vulnerability
CVE-2018-8392 - Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2018-8393 - Microsoft JET Database Engine Remote Code Execution Vulnerability
CVE-2018-8426 - Microsoft Office SharePoint XSS Vulnerability
CVE-2018-8428 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8431 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2018-8434 - Windows Hyper-V Information Disclosure Vulnerability
CVE-2018-8435 - Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2018-8436 - Windows Hyper-V Denial of Service Vulnerability
CVE-2018-8437 - Windows Hyper-V Denial of Service Vulnerability
CVE-2018-8438 - Windows Hyper-V Denial of Service Vulnerability
CVE-2018-8439 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2018-8440 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2018-8441 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2018-8442 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8443 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8444 - Windows SMB Information Disclosure Vulnerability
CVE-2018-8445 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8446 - Windows Kernel Information Disclosure Vulnerability
CVE-2018-8449 - Device Guard Security Feature Bypass Vulnerability
CVE-2018-8455 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2018-8468 - Windows Elevation of Privilege Vulnerability
CVE-2018-8474 - Lync for Mac 2011 Security Feature Bypass Vulnerability
CVE-2018-8479 - Azure IoT SDK Spoofing Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Microsoft.Data.OData
Windows 10 Version 1803 for x64-based Systems
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
ChakraCore
Microsoft SharePoint Server 2010 Service Pack 2
Windows 8.1 for 32-bit systems
Microsoft Lync for Mac 2011
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Server, version 1803 (Server Core Installation)
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
C SDK for Azure IoT
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8424
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8439
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8337
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8426
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8391
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8475
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8479

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8446
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8435
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8438
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8422
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8392
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8474
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8419
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8462
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8437
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8455
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8443
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8440
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8271
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8468
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8445
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8269
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8428
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8433
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8393
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0965
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8434
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8449
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8336
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8442

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8431
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8441
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8444
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8335
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8410
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8420
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8436
BUGTRAQ	http://www.securityfocus.com/bid/105233
BUGTRAQ	http://www.securityfocus.com/bid/105277
BUGTRAQ	http://www.securityfocus.com/bid/105217
BUGTRAQ	http://www.securityfocus.com/bid/105357
BUGTRAQ	http://www.securityfocus.com/bid/105213
BUGTRAQ	http://www.securityfocus.com/bid/105268
BUGTRAQ	http://www.securityfocus.com/bid/105211
BUGTRAQ	http://www.securityfocus.com/bid/105275
BUGTRAQ	http://www.securityfocus.com/bid/105264
BUGTRAQ	http://www.securityfocus.com/bid/105214
BUGTRAQ	http://www.securityfocus.com/bid/105272
BUGTRAQ	http://www.securityfocus.com/bid/105226
BUGTRAQ	http://www.securityfocus.com/bid/105259
BUGTRAQ	http://www.securityfocus.com/bid/105239
BUGTRAQ	http://www.securityfocus.com/bid/105153
BUGTRAQ	http://www.securityfocus.com/bid/105274
BUGTRAQ	http://www.securityfocus.com/bid/105323

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/105261
BUGTRAQ	http://www.securityfocus.com/bid/105221
BUGTRAQ	http://www.securityfocus.com/bid/105250
BUGTRAQ	http://www.securityfocus.com/bid/105208
BUGTRAQ	http://www.securityfocus.com/bid/105231
BUGTRAQ	http://www.securityfocus.com/bid/105240
BUGTRAQ	http://www.securityfocus.com/bid/105249
BUGTRAQ	http://www.securityfocus.com/bid/105238
BUGTRAQ	http://www.securityfocus.com/bid/105237
BUGTRAQ	http://www.securityfocus.com/bid/105228
BUGTRAQ	http://www.securityfocus.com/bid/105247
BUGTRAQ	http://www.securityfocus.com/bid/105225
BUGTRAQ	http://www.securityfocus.com/bid/105322
BUGTRAQ	http://www.securityfocus.com/bid/105209
BUGTRAQ	http://www.securityfocus.com/bid/105229
BUGTRAQ	http://www.securityfocus.com/bid/105246
BUGTRAQ	http://www.securityfocus.com/bid/105234
BUGTRAQ	http://www.securityfocus.com/bid/105271
BUGTRAQ	http://www.securityfocus.com/bid/105224
BUGTRAQ	http://www.securityfocus.com/bid/105256
BUGTRAQ	http://www.securityfocus.com/bid/105236
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8428
URL	https://support.microsoft.com/en-us/help/4457132
URL	https://support.microsoft.com/en-us/help/4457138

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8424
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8439
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8337
URL	https://cwe.mitre.org/data/definitions/611.html
URL	https://cwe.mitre.org/data/definitions/295.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://blog.0patch.com/2018/09/comparing-our-micropatch-with.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://blog.0patch.com/2018/08/how-we-micropatched-publicly-dropped.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8426
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8391
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8475
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8479
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8446
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8435
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8438
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8422
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8392

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8474
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8419
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8462
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8437
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8455
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8443
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8440
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8271
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8468
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8445
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8269
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180022
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8433
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8393
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0965

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8434
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8449
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8336
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8442
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8431
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8441
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8444
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8335
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8410
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8420
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8436
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/190.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://support.microsoft.com/en-us/help/4457140
URL	https://support.microsoft.com/en-us/help/4457145
URL	https://support.microsoft.com/en-us/help/4457143

Type	Reference
URL	https://support.microsoft.com/en-us/help/4092470
URL	https://support.microsoft.com/en-us/help/4022207
URL	https://support.microsoft.com/en-us/help/4092459
URL	https://support.microsoft.com/en-us/help/4457984
URL	https://support.microsoft.com/en-us/help/4457144
URL	https://support.microsoft.com/en-us/help/4457135
URL	https://support.microsoft.com/en-us/help/4457142
URL	https://support.microsoft.com/en-us/help/4457129
URL	https://support.microsoft.com/en-us/help/4457131
URL	https://support.microsoft.com/en-us/help/4458010
URL	https://support.microsoft.com/en-us/help/4457128

MS19-APR: Microsoft Internet Explorer Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-0764 - Microsoft Browsers Tampering Vulnerability
CVE-2019-0752 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-0753 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-0835 - Microsoft Scripting Engine Information Disclosure Vulnerability
CVE-2019-0862 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems

Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Microsoft Edge on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

Solution Details

Microsoft has released a fix for this flaw in their April 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0835

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0753
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0862
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0764
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0752
BUGTRAQ	http://www.securityfocus.com/bid/107727
BUGTRAQ	http://www.securityfocus.com/bid/107731
URL	http://packetstormsecurity.com/files/153078/Microsoft-Internet-Explorer-Windows-10-1809-17763.316-Memory-Corruption.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0835
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0753
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0862
URL	https://support.microsoft.com/en-us/help/4493435
URL	https://support.microsoft.com/en-us/help/4493446
URL	https://support.microsoft.com/en-us/help/4493509
URL	https://support.microsoft.com/en-us/help/4493472
URL	https://support.microsoft.com/en-us/help/4493441
URL	https://support.microsoft.com/en-us/help/4493474
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-359/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0752
URL	https://support.microsoft.com/en-us/help/4493475
URL	https://support.microsoft.com/en-us/help/4493451

Type	Reference
URL	https://support.microsoft.com/en-us/help/4493470
URL	https://support.microsoft.com/en-us/help/4493464
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4493471
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0764

MS19-APR: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-0790 - MS XML Remote Code Execution Vulnerability
CVE-2019-0791 - MS XML Remote Code Execution Vulnerability
CVE-2019-0792 - MS XML Remote Code Execution Vulnerability
CVE-2019-0793 - MS XML Remote Code Execution Vulnerability
CVE-2019-0794 - OLE Automation Remote Code Execution Vulnerability
CVE-2019-0795 - MS XML Remote Code Execution Vulnerability
CVE-2019-0802 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0803 - Win32k Elevation of Privilege Vulnerability
CVE-2019-0805 - Windows Elevation of Privilege Vulnerability
CVE-2019-0815 - ASP.NET Core Denial of Service Vulnerability
CVE-2019-0830 - Microsoft Office SharePoint XSS Vulnerability
CVE-2019-0831 - Microsoft Office SharePoint XSS Vulnerability
CVE-2019-0838 - Windows Information Disclosure Vulnerability
CVE-2019-0839 - Windows Information Disclosure Vulnerability
CVE-2019-0840 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0841 - Windows Elevation of Privilege Vulnerability
CVE-2019-0842 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2019-0844 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0845 - Windows IOleCvt Interface Remote Code Execution Vulnerability
CVE-2019-0846 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0847 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0848 - Win32k Information Disclosure Vulnerability
CVE-2019-0849 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0851 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0853 - GDI+ Remote Code Execution Vulnerability
CVE-2019-0877 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0879 - Jet Database Engine Remote Code Execution Vulnerability
ADV990001 - Latest Servicing Stack Updates

CVE-2019-0685 - Win32k Elevation of Privilege Vulnerability
CVE-2019-0688 - Windows TCP/IP Information Disclosure Vulnerability
CVE-2019-0730 - Windows Elevation of Privilege Vulnerability
CVE-2019-0731 - Windows Elevation of Privilege Vulnerability
CVE-2019-0732 - Windows Security Feature Bypass Vulnerability
CVE-2019-0735 - Windows CSRSS Elevation of Privilege Vulnerability
CVE-2019-0786 - SMB Server Elevation of Privilege Vulnerability
CVE-2019-0796 - Windows Elevation of Privilege Vulnerability
CVE-2019-0813 - Windows Admin Center Elevation of Privilege Vulnerability
CVE-2019-0814 - Win32k Information Disclosure Vulnerability
CVE-2019-0836 - Windows Elevation of Privilege Vulnerability
CVE-2019-0837 - DirectX Information Disclosure Vulnerability
CVE-2019-0856 - Windows Remote Code Execution Vulnerability
CVE-2019-0857 - Azure DevOps Server Spoofing Vulnerability
CVE-2019-0859 - Win32k Elevation of Privilege Vulnerability
CVE-2019-0866 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-0867 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-0868 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-0869 - Azure DevOps Server HTML Injection Vulnerability
CVE-2019-0870 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-0871 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-0874 - Azure DevOps Server Cross-site Scripting Vulnerability
CVE-2019-0875 - Azure DevOps Server Elevation of Privilege Vulnerability
CVE-2019-0876 - Open Enclave SDK Information Disclosure Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Admin Center
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Open Enclave SDK
ASP.NET Core 2.2
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Microsoft SharePoint Server 2010 Service Pack 2
Windows 8.1 for 32-bit systems

Team Foundation Server 2018 Updated 1.2
Team Foundation Server 2017 Update 3.1
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Team Foundation Server 2018 Update 3.2
Windows 10 Version 1803 for 32-bit Systems
Azure DevOps Server 2019
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Server, version 1803 (Server Core Installation)
Microsoft SharePoint Foundation 2010 Service Pack 2
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Microsoft SharePoint Foundation 2013 Service Pack 1
Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Team Foundation Server 2015 Update 4.2
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft SharePoint Server 2019
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their April 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0879
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0792
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0795

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0815
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0849
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0790
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0857
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0844
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0868
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0848
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0837
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0802
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0841
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0847
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0805
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0842
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0791
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0876
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0731
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0875
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0840
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0796
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0688
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0845
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0830
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0793
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0803

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0814
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0831
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0859
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0836
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0732
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0869
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0856
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0874
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0735
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0730
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0846
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0877
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0851
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0871
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0866
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0838
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0794
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0853
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0867
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0813
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0839
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0870
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0786
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0685

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/107741
BUGTRAQ	http://www.securityfocus.com/bid/107728
BUGTRAQ	http://www.securityfocus.com/bid/107732
BUGTRAQ	http://www.securityfocus.com/bid/107701
BUGTRAQ	http://www.securityfocus.com/bid/107702
BUGTRAQ	http://www.securityfocus.com/bid/107760
BUGTRAQ	http://www.securityfocus.com/bid/107753
BUGTRAQ	http://www.securityfocus.com/bid/107725
BUGTRAQ	http://www.securityfocus.com/bid/107726
BUGTRAQ	http://www.securityfocus.com/bid/107743
BUGTRAQ	http://www.securityfocus.com/bid/107729
BUGTRAQ	http://www.securityfocus.com/bid/107719
BUGTRAQ	http://www.securityfocus.com/bid/107768
BUGTRAQ	http://www.securityfocus.com/bid/107759
BUGTRAQ	http://www.securityfocus.com/bid/107755
BUGTRAQ	http://www.securityfocus.com/bid/107749
BUGTRAQ	http://www.securityfocus.com/bid/107752
BUGTRAQ	http://www.securityfocus.com/bid/107754
BUGTRAQ	http://www.securityfocus.com/bid/107685
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0796
URL	https://support.microsoft.com/en-us/help/4493467
URL	https://support.microsoft.com/en-us/help/4485447
URL	https://support.microsoft.com/en-us/help/4493448
URL	https://support.microsoft.com/en-us/help/4464525

Type	Reference
URL	https://support.microsoft.com/en-us/help/4464518
URL	https://support.microsoft.com/en-us/help/4464515
URL	https://support.microsoft.com/en-us/help/4493730
URL	https://support.microsoft.com/en-us/help/4464510
URL	https://support.microsoft.com/en-us/help/4493450
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0870
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0839
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0813
URL	https://support.microsoft.com/en-us/help/4485449
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0853
URL	https://support.microsoft.com/en-us/help/4464528
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0794
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0838
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0866
URL	http://packetstormsecurity.com/files/152538/Microsoft-Windows-LUAFV-PostLuafvPostReadWrite-SECTION_OBJECT_POINTERS-Race-Condition.html
URL	http://packetstormsecurity.com/files/152536/Microsoft-Windows-LUAFV-NtSetCachedSigningLevel-Device-Guard-Bypass.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0871

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0851
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0877
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0846
URL	https://support.microsoft.com/en-us/help/4464511
URL	http://packetstormsecurity.com/files/152532/Microsoft-Windows-CSRSS-SxSSrv-Cached-Manifest-Privilege-Escalation.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0786
URL	https://support.microsoft.com/en-us/help/4493458
URL	https://support.microsoft.com/en-us/help/4493552
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001
URL	https://support.microsoft.com/en-us/help/4490628
URL	https://support.microsoft.com/en-us/help/4487327
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0867
URL	https://support.microsoft.com/en-us/help/3173424
URL	https://support.microsoft.com/en-us/help/4093430
URL	https://support.microsoft.com/en-us/help/4485448
URL	https://support.microsoft.com/en-us/help/3173426
URL	https://support.microsoft.com/en-us/help/4493510
URL	http://packetstormsecurity.com/files/152533/Microsoft-Windows-LUAFV-Delayed-Virtualization-MAXIMUM_ACCESS-DesiredAccess-Privilege-Escalation.html
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-362/
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-363/

Type	Reference
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/74.html
URL	https://cwe.mitre.org/data/definitions/611.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	http://packetstormsecurity.com/files/152463/Microsoft-Windows-AppX-Deployment-Service-Privilege-Escalation.html
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-360/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0730
URL	http://packetstormsecurity.com/files/152537/Microsoft-Windows-LUAFV-Delayed-Virtualization-Cache-Manager-Poisoning-Privilege-Escalation.html
URL	http://packetstormsecurity.com/files/152534/Microsoft-Windows-LUAFV-Delayed-Virtualization-Cross-Process-Handle-Duplication-Privilege-Escalation.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0735
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0874
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0856
URL	http://packetstormsecurity.com/files/152535/Microsoft-Windows-LUAFV-LuafvCopyShortName-Arbitrary-Short-Name-Privilege-Escalation.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0869
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0732
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0836

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0859
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0831
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0814
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0803
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0793
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0830
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0845
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0688
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0840
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0875
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0731
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0876
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0791
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0842
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0805
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0847

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0841
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0802
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0837
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0848
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0868
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0844
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0857
URL	https://arxiv.org/pdf/1906.10478.pdf
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0790
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0849
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0815
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0795
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0792
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0879
URL	https://support.microsoft.com/en-us/help/4493471
URL	https://support.microsoft.com/en-us/help/4493464
URL	https://support.microsoft.com/en-us/help/4493470
URL	https://support.microsoft.com/en-us/help/4493451

Type	Reference
URL	https://support.microsoft.com/en-us/help/4493475
URL	https://support.microsoft.com/en-us/help/4493474
URL	https://support.microsoft.com/en-us/help/4493441
URL	https://support.microsoft.com/en-us/help/4493472
URL	https://support.microsoft.com/en-us/help/4493509
URL	https://support.microsoft.com/en-us/help/4493446
URL	http://packetstormsecurity.com/files/153009/Internet-Explorer-JavaScript-Privilege-Escalation.html
URL	http://packetstormsecurity.com/files/153034/Microsoft-Windows-Win32k-Privilege-Escalation.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0685
URL	http://packetstormsecurity.com/files/153114/Microsoft-Windows-AppX-Deployment-Service-Local-Privilege-Escalation.html
URL	http://packetstormsecurity.com/files/153215/Microsoft-Windows-AppX-Deployment-Service-Local-Privilege-Escalation.html

MS19-AUG: Microsoft Internet Explorer Security Update — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-1133 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1192 - Microsoft Browsers Security Feature Bypass Vulnerability
CVE-2019-1193 - Microsoft Browser Memory Corruption Vulnerability
CVE-2019-1194 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems

Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Microsoft Edge on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems

Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

Solution Details

Microsoft has released a fix for this flaw in their August 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1133
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1192
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1194
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1193
URL	https://support.microsoft.com/en-us/help/4512508
URL	https://support.microsoft.com/en-us/help/4511553
URL	https://support.microsoft.com/en-us/help/4512518
URL	https://support.microsoft.com/en-us/help/4512497
URL	https://support.microsoft.com/en-us/help/4512488
URL	https://support.microsoft.com/en-us/help/4512506
URL	https://support.microsoft.com/en-us/help/4512507
URL	https://support.microsoft.com/en-us/help/4512516
URL	https://support.microsoft.com/en-us/help/4512517
URL	https://support.microsoft.com/en-us/help/4512501
URL	https://support.microsoft.com/en-us/help/4511872
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1133
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1193

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1194
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1192
URL	https://support.microsoft.com/en-us/help/4512476

MS19-AUG: Microsoft Windows Security Update

High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-0965 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-1057 - MS XML Remote Code Execution Vulnerability
CVE-2019-9506 - Encryption Key Negotiation of Bluetooth Vulnerability
CVE-2019-1171 - SymCrypt Information Disclosure Vulnerability
CVE-2019-1172 - Windows Information Disclosure Vulnerability
CVE-2019-1173 - Windows Elevation of Privilege Vulnerability
CVE-2019-1174 - Windows Elevation of Privilege Vulnerability
CVE-2019-1175 - Windows Elevation of Privilege Vulnerability
CVE-2019-1178 - Windows Elevation of Privilege Vulnerability
CVE-2019-1179 - Windows Elevation of Privilege Vulnerability
CVE-2019-1180 - Windows Elevation of Privilege Vulnerability
CVE-2019-1181 - Remote Desktop ServicesÂ Remote Code Execution Vulnerability
CVE-2019-1182 - Remote Desktop ServicesÂ Remote Code Execution Vulnerability
CVE-2019-1183 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2019-1206 - Windows DHCP Server Denial of Service Vulnerability
CVE-2019-0714 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0715 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0716 - Windows Denial of Service Vulnerability
CVE-2019-0717 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0718 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0720 - Hyper-V Remote Code Execution Vulnerability
CVE-2019-0723 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0736 - Windows DHCP Client Remote Code Execution Vulnerability
CVE-2019-1078 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2019-1143 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2019-1144 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2019-1145 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2019-1146 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1147 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1150 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2019-1152 - Microsoft Graphics Remote Code Execution Vulnerability

CVE-2019-1154 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2019-1156 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1157 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1158 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2019-1159 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1161 - Microsoft Defender Elevation of Privilege Vulnerability
CVE-2019-1162 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2019-1163 - Windows File Signature Security Feature Bypass Vulnerability
CVE-2019-1164 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1168 - Microsoft Windows p2pimsvc Elevation of Privilege Vulnerability
CVE-2019-1169 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1170 - Windows NTFS Elevation of Privilege Vulnerability
CVE-2019-1176 - DirectX Elevation of Privilege Vulnerability
CVE-2019-1177 - Windows Elevation of Privilege Vulnerability
CVE-2019-1184 - Windows Elevation of Privilege Vulnerability
CVE-2019-1185 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-1186 - Windows Elevation of Privilege Vulnerability
CVE-2019-1187 - XmlLite Runtime Denial of Service Vulnerability
CVE-2019-1190 - Windows Image Elevation of Privilege Vulnerability
ADV190023 - Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing
CVE-2019-1188 - LNK Remote Code Execution Vulnerability
CVE-2019-1198 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-9511 - HTTP/2 Server Denial of Service Vulnerability
CVE-2019-9512 - HTTP/2 Server Denial of Service Vulnerability
CVE-2019-9513 - HTTP/2 Server Denial of Service Vulnerability
CVE-2019-9514 - HTTP/2 Server Denial of Service Vulnerability
CVE-2019-1211 - Git for Visual Studio Elevation of Privilege Vulnerability
CVE-2019-1212 - Windows DHCP Server Denial of Service Vulnerability
CVE-2019-1213 - Windows DHCP Server Remote Code Execution Vulnerability
CVE-2019-9518 - HTTP/2 Server Denial of Service Vulnerability
CVE-2019-1222 - Remote Desktop ServicesÂ Remote Code Execution Vulnerability
CVE-2019-1223 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2019-1224 - Remote Desktop Protocol Server Information Disclosure Vulnerability
CVE-2019-1225 - Remote Desktop Protocol Server Information Disclosure Vulnerability
CVE-2019-1226 - Remote Desktop ServicesÂ Remote Code Execution Vulnerability
CVE-2019-1227 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-1228 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-1229 - Dynamics On-Premise Elevation of Privilege Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows Defender on Windows Server 2012
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)

Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
Windows Defender on Windows Server 2016 (Server Core installation)
Microsoft System Center 2012 R2 Endpoint Protection
Windows Defender on Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1703 for x64-based Systems
Microsoft Visual Studio 2017 version 15.9
Windows Defender on Windows Server 2016
Windows 8.1 for x64-based systems
Windows Defender on Windows 7 for 32-bit Systems Service Pack 1
Microsoft Visual Studio 2017
Windows 10 Version 1903 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.2
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Security Essentials
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1903 for ARM64-based Systems
Windows Defender on Windows 10 for 32-bit Systems
Windows Defender on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Defender on Windows 10 for x64-based Systems
Windows 10 Version 1809 for x64-based Systems
Microsoft System Center 2012 Endpoint Protection
Microsoft Forefront Endpoint Protection 2010
Windows Defender on Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1703 for x64-based Systems
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Defender on Windows 10 Version 1607 for 32-bit Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1607 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for 32-bit Systems

Windows Defender on Windows 8.1 for x64-based systems
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft Dynamics 365 (on-premises) version 9.0
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Windows Defender on Windows Server 2012 R2
Windows 10 Version 1803 for ARM64-based Systems
Microsoft System Center Endpoint Protection
Windows Defender on Windows Server 2012 (Server Core installation)
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Defender on Windows 10 Version 1703 for 32-bit Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows 7 for x64-based Systems Service Pack 1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their August 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1190
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0723
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0718
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1161
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1146
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1172
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1227
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1156

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1222
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1169
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1147
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1171
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0720
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9513
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1182
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9514
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1212
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1057
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1228
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1206
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1152
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0736
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9506
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1183
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1224
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1181
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1226
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1168
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1174
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0717
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1159
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1229

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1150
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1154
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1175
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1177
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9512
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1185
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1164
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1178
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1223
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9518
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1179
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0716
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1144
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1187
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0714
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0965
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1213
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1180
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1158
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1173
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0715
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1163
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1186
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1211

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1078
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1225
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1143
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1184
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9511
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1157
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1170
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1198
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1188
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1176
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1162
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1229
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1223
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-9518
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1206
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1228
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1179
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0716
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1144

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1187
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0714
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0965
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1213
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1180
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1158
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1173
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0715
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1163
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1186
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1211
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1078
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1225
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1143
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1184
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-9511

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1145
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1157
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1170
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1057
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1212
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1198
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0736
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1188
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1176
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1162
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-9514
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1177
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-9513
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1178

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1164
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1185
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-9512
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1190
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1175
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1154
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1150
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1168
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181
URL	https://support.microsoft.com/en-us/help/4512476
URL	https://support.microsoft.com/en-us/help/4512501
URL	https://support.microsoft.com/en-us/help/4512517
URL	https://support.microsoft.com/en-us/help/4512516
URL	https://support.microsoft.com/en-us/help/4512507
URL	https://support.microsoft.com/en-us/help/4512506
URL	https://support.microsoft.com/en-us/help/4512488
URL	https://support.microsoft.com/en-us/help/4512497
URL	https://support.microsoft.com/en-us/help/4512518

Type	Reference
URL	https://support.microsoft.com/en-us/help/4511553
URL	https://support.microsoft.com/en-us/help/4512508
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1224
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1183
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0720
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1171
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1147
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1169
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1156
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1227
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-9506
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1172
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1146
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1161
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0718

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0723
URL	https://support.microsoft.com/en-us/help/4512489
URL	https://support.microsoft.com/en-us/help/4512482
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1152
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0717
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1159
URL	https://support.microsoft.com/en-us/help/4512486
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1174
URL	https://support.microsoft.com/en-us/help/4508724
URL	https://support.microsoft.com/en-us/help/4512491

MS19-DEC: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their December 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-1485 - VBScript Remote Code Execution Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems

Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1485
URL	https://support.microsoft.com/en-us/help/4530677
URL	https://support.microsoft.com/en-us/help/4530691
URL	https://support.microsoft.com/en-us/help/4530689
URL	https://support.microsoft.com/en-us/help/4530717
URL	https://support.microsoft.com/en-us/help/4530715
URL	https://support.microsoft.com/en-us/help/4530734

Type	Reference
URL	https://support.microsoft.com/en-us/help/4530684
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1485
URL	https://support.microsoft.com/en-us/help/4530714
URL	https://support.microsoft.com/en-us/help/4530681
URL	https://support.microsoft.com/en-us/help/4530702
URL	https://support.microsoft.com/en-us/help/4530695

MS19-DEC: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-1453 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2019-1470 - Windows Hyper-V Information Disclosure Vulnerability
CVE-2019-1471 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-1472 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-1474 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-1480 - Windows Media Player Information Disclosure Vulnerability
CVE-2019-1481 - Windows Media Player Information Disclosure Vulnerability
CVE-2019-1483 - Windows Elevation of Privilege Vulnerability
CVE-2019-1484 - Windows OLE Remote Code Execution Vulnerability
CVE-2019-1487 - Microsoft Authentication Library for Android Information Disclosure Vulnerability
CVE-2019-1488 - Microsoft Defender Security Feature Bypass Vulnerability
CVE-2019-1489 - Remote Desktop Protocol Information Disclosure Vulnerability
ADV990001 - Latest Servicing Stack Updates
CVE-2019-1349 - Git for Visual Studio Remote Code Execution Vulnerability
CVE-2019-1350 - Git for Visual Studio Remote Code Execution Vulnerability
CVE-2019-1351 - Git for Visual Studio Tampering Vulnerability
CVE-2019-1352 - Git for Visual Studio Remote Code Execution Vulnerability
CVE-2019-1354 - Git for Visual Studio Remote Code Execution Vulnerability
CVE-2019-1387 - Git for Visual Studio Remote Code Execution Vulnerability
CVE-2019-1458 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1465 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1466 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1467 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1468 - Win32k Graphics Remote Code Execution Vulnerability
CVE-2019-1469 - Win32k Information Disclosure Vulnerability
CVE-2019-1476 - Windows Elevation of Privilege Vulnerability

CVE-2019-1477 - Windows Printer Service Elevation of Privilege Vulnerability
CVE-2019-1478 - Windows COM Server Elevation of Privilege Vulnerability
ADV190026 - Microsoft Guidance for cleaning up orphaned keys generated on vulnerable TPMs and used for Windows Hello for Business
CVE-2019-1486 - Visual Studio Live Share Spoofing Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Microsoft Visual Studio 2019 version 16.0
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Microsoft Windows XP Service Pack 3
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Server, version 1909 (Server Core installation)
Windows 10 Version 1909 for x64-based Systems
Microsoft Visual Studio Live Share extension
Windows 10 Version 1903 for 32-bit Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Microsoft Visual Studio 2017 version 16.0
Windows 10 Version 1909 for 32-bit Systems
Microsoft Authentication Library (MSAL) for Android

Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Microsoft Visual Studio 2017 version 15.0
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
None Available

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their December 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1481
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1478
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1483
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1387
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1471
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1466
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1480
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1354
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1465
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1468
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1458
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1488
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1352

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1467
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1484
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1472
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1470
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1474
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1489
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1476
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1486
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1487
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1349
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1350
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1453
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1351
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1477
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1469
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1477
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-1003/
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-1005/
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-1002/
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-1007/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-1008/
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-1004/

Type	Reference
URL	https://support.microsoft.com/en-us/help/4530719
URL	https://support.microsoft.com/en-us/help/4530692
URL	https://support.microsoft.com/en-us/help/4530698
URL	https://support.microsoft.com/en-us/help/4530730
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1352
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190026
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1467
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1484
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1472
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1470
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1474
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1489
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1476
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1486
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1487
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1349
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1350

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1453
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1351
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1469
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1488
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1481
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1478
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1483
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1387
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1471
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1466
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1480
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1354
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1465
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1468
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1458
URL	https://support.microsoft.com/en-us/help/4530715

Type	Reference
URL	https://support.microsoft.com/en-us/help/4530734
URL	https://support.microsoft.com/en-us/help/4530717
URL	https://support.microsoft.com/en-us/help/4530681
URL	https://support.microsoft.com/en-us/help/4530684
URL	https://support.microsoft.com/en-us/help/4530695
URL	https://support.microsoft.com/en-us/help/4530714
URL	https://support.microsoft.com/en-us/help/4530689
URL	https://support.microsoft.com/en-us/help/4530691
URL	https://support.microsoft.com/en-us/help/4530702
URL	https://support.microsoft.com/en-us/help/4523206
URL	https://support.microsoft.com/en-us/help/4526478
URL	https://support.microsoft.com/en-us/help/4524569
URL	https://support.microsoft.com/en-us/help/4523202
URL	https://support.microsoft.com/en-us/help/4523200
URL	https://support.microsoft.com/en-us/help/4520724
URL	https://support.microsoft.com/en-us/help/4523208
URL	https://support.microsoft.com/en-us/help/4524445
URL	https://support.microsoft.com/en-us/help/4523203
URL	https://support.microsoft.com/en-us/help/4523204

MS19-FEB: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their February 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-0606 - Internet Explorer Memory Corruption Vulnerability
CVE-2019-0654 - Microsoft Browser Spoofing Vulnerability
CVE-2019-0676 - Internet Explorer Information Disclosure Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Microsoft Edge on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012 R2

Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0676
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0606
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0654
BUGTRAQ	http://www.securityfocus.com/bid/106881
BUGTRAQ	http://www.securityfocus.com/bid/106859
BUGTRAQ	http://www.securityfocus.com/bid/106886
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://support.microsoft.com/en-us/help/4487044
URL	https://support.microsoft.com/en-us/help/4487023
URL	https://support.microsoft.com/en-us/help/4486563
URL	https://support.microsoft.com/en-us/help/4486474
URL	https://support.microsoft.com/en-us/help/4487025
URL	https://support.microsoft.com/en-us/help/4487017
URL	https://support.microsoft.com/en-us/help/4486996
URL	https://support.microsoft.com/en-us/help/4487018
URL	https://support.microsoft.com/en-us/help/4487020
URL	https://support.microsoft.com/en-us/help/4487026
URL	https://support.microsoft.com/en-us/help/4487000

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0606
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0654
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0676
URL	https://cwe.mitre.org/data/definitions/20.html

MS19-FEB: Microsoft Windows Security Update High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-0623 - Win32k Elevation of Privilege Vulnerability
CVE-2019-0625 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0628 - Win32k Information Disclosure Vulnerability
CVE-2019-0656 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-0659 - Windows Storage Service Elevation of Privilege Vulnerability
CVE-2019-0660 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0661 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0662 - GDI+ Remote Code Execution Vulnerability
CVE-2019-0664 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0668 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2019-0670 - Microsoft SharePoint Spoofing Vulnerability
ADV190004 - February 2019 Oracle Outside In Library Security Update
CVE-2019-0729 - Azure IoT Java SDK Elevation of Privilege Vulnerability
CVE-2019-0741 - Azure IoT Java SDK Information Disclosure Vulnerability
CVE-2019-0743 - Team Foundation Server Cross-site Scripting Vulnerability
ADV990001 - Latest Servicing Stack Updates
CVE-2019-0594 - Microsoft SharePoint Remote Code Execution Vulnerability
CVE-2019-0595 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0596 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0597 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0598 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0599 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0600 - HID Information Disclosure Vulnerability
CVE-2019-0601 - HID Information Disclosure Vulnerability

CVE-2019-0602 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0604 - Microsoft SharePoint Remote Code Execution Vulnerability
CVE-2019-0615 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0616 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0618 - GDI+ Remote Code Execution Vulnerability
CVE-2019-0619 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0621 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0626 - Windows DHCP Server Remote Code Execution Vulnerability
CVE-2019-0627 - Windows Security Feature Bypass Vulnerability
CVE-2019-0630 - Windows SMB Remote Code Execution Vulnerability
CVE-2019-0631 - Windows Security Feature Bypass Vulnerability
CVE-2019-0632 - Windows Security Feature Bypass Vulnerability
CVE-2019-0633 - Windows SMB Remote Code Execution Vulnerability
CVE-2019-0635 - Windows Hyper-V Information Disclosure Vulnerability
CVE-2019-0636 - Windows Information Disclosure Vulnerability
CVE-2019-0637 - Windows Defender Firewall Security Feature Bypass Vulnerability
CVE-2019-0686 - Microsoft Exchange Server Elevation of Privilege Vulnerability
CVE-2019-0724 - Microsoft Exchange Server Elevation of Privilege Vulnerability
ADV190006 - Guidance to mitigate unconstrained delegation vulnerabilities
CVE-2019-0728 - Visual Studio Code Remote Code Execution Vulnerability
ADV190007 - Guidance for "PrivExchange" Elevation of Privilege Vulnerability
CVE-2019-0742 - Team Foundation Server Cross-site Scripting Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 26
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 for 32-bit Systems
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Microsoft Exchange Server 2013 Cumulative Update 22
Windows 10 Version 1803 for x64-based Systems
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Microsoft Exchange Server 2019 Cumulative Update 1
Windows Server 2012 R2
Microsoft SharePoint Server 2010 Service Pack 2
Windows 8.1 for 32-bit systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1

Java SDK for Azure IoT
Team Foundation Server 2018 Update 3.2
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Microsoft Exchange Server 2016 Cumulative Update 12
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2016 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft SharePoint Foundation 2013 Service Pack 1
Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft SharePoint Server 2019
Windows Server, version 1709 (Server Core Installation)

Solution Details

Microsoft has released a fix for this flaw in their February 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0676
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0729
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0597
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190003
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0540

Type	Reference
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0598
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0599
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0743
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0595
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0594
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0600
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0604
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190006
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0669
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0658
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0648
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0618
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0643
URL	https://support.microsoft.com/en-us/help/4345836/cumulative-update-22-for-exchange-server-2013
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0631
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0728

Type	Reference
URL	https://support.microsoft.com/en-us/help/4471391/cumulative-update-1-for-exchange-server-2019
URL	https://support.microsoft.com/en-us/help/4471392/cumulative-update-12-for-exchange-server-2016
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0601
URL	https://support.microsoft.com/en-us/help/4486563/windows-7-update-kb4486563
URL	https://support.microsoft.com/en-us/help/4486564/windows-7-update-kb4486564
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0660
URL	https://support.microsoft.com/en-us/help/4486993/windows-server-2012-update-kb4486993
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0661
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0664
URL	https://support.microsoft.com/en-us/help/4487000/windows-8-1-update-kb4487000
URL	https://support.microsoft.com/en-us/help/4487019/windows-server-2008-update-kb4487019
URL	https://support.microsoft.com/en-us/help/4487020/windows-10-update-kb4487020
URL	https://support.microsoft.com/en-us/help/4487023/windows-server-2008-update-kb4487023
URL	https://support.microsoft.com/en-us/help/4487025/windows-server-2012-update-kb4487025
URL	https://support.microsoft.com/en-us/help/4487026/windows-10-update-kb4487026
URL	https://support.microsoft.com/en-us/help/4487028/windows-8-1-update-kb4487028

Type	Reference
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0630
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0686
URL	https://support.microsoft.com/en-us/help/4486996/windows-10-update-kb4486996
URL	https://support.microsoft.com/en-us/help/4487017/windows-10-update-kb4487017
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0615
URL	https://support.microsoft.com/en-us/help/4487044/windows-10-update-kb4487044
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0602
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0724
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0627
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0626
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0741
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0616
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0619
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0623
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0621
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0742

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190007
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0625
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0656
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0659
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0633
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0662
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0632
URL	https://support.microsoft.com/en-us/help/4487052/update-rollup-26-for-exchange-server-2010-service-p
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0668
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0670
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0628
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0596
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0637
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0635
URL	https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-0636

MS19-JAN: Microsoft Windows Security Update

High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-0538 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0536 - Windows Kernel Information Disclosure Vulnerability
ADV990001 - Latest Servicing Stack Updates
CVE-2019-0537 - Microsoft Visual Studio Information Disclosure Vulnerability
CVE-2019-0546 - Visual Studio Remote Code Execution Vulnerability
CVE-2019-0543 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-0547 - Windows DHCP Client Remote Code Execution Vulnerability
CVE-2019-0549 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0550 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-0551 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-0552 - Windows COM Elevation of Privilege Vulnerability
CVE-2019-0553 - Windows Subsystem for Linux Information Disclosure Vulnerability
CVE-2019-0554 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0555 - Microsoft XmlDocument Elevation of Privilege Vulnerability
CVE-2019-0556 - Microsoft Office SharePoint XSS Vulnerability
CVE-2019-0557 - Microsoft Office SharePoint XSS Vulnerability
CVE-2019-0558 - Microsoft Office SharePoint XSS Vulnerability
CVE-2019-0562 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2019-0569 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0570 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2019-0571 - Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2019-0572 - Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2019-0573 - Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2019-0574 - Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2019-0575 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0576 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0577 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0578 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0579 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0580 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0581 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0582 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0583 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0584 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0586 - Microsoft Exchange Memory Corruption Vulnerability
CVE-2019-0588 - Microsoft Exchange Information Disclosure Vulnerability
CVE-2019-0622 - Skype for Android Elevation of Privilege Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems

Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 25
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Microsoft Business Productivity Servers 2010 Service Pack 2
Windows 10 Version 1803 for x64-based Systems
Microsoft Exchange Server 2016 Cumulative Update 11
Microsoft SharePoint Enterprise Server 2013 Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Microsoft Visual Studio 2012 Update 5
Windows 8.1 for 32-bit systems
Microsoft Exchange Server 2013 Cumulative Update 21
Microsoft Exchange Server 2019
Microsoft Exchange Server 2016 Cumulative Update 10
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Microsoft Visual Studio 2010 Service Pack 1
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1803 for ARM64-based Systems
Skype 8.35 when installed on Android Devices
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft SharePoint Server 2019
Windows Server, version 1709 (Server Core Installation)

Solution Details

Microsoft has released a fix for this flaw in their January 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0577
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0552
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0569
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0574
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0572
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0555
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0547
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0538
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0562
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0536
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0580
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0622
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0570
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0573
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0582
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0581
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0550
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0578

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0551
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0583
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0586
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0553
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0588
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0579
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0584
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0554
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0543
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0556
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0546
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0549
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0575
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0576
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0557
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0537
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0571
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0558
BUGTRAQ	http://www.securityfocus.com/bid/106389
BUGTRAQ	http://www.securityfocus.com/bid/106426
BUGTRAQ	http://www.securityfocus.com/bid/106390
BUGTRAQ	http://www.securityfocus.com/bid/106388
BUGTRAQ	http://www.securityfocus.com/bid/106422
BUGTRAQ	http://www.securityfocus.com/bid/106404

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/106409
BUGTRAQ	http://www.securityfocus.com/bid/106391
BUGTRAQ	http://www.securityfocus.com/bid/106387
BUGTRAQ	http://www.securityfocus.com/bid/106408
BUGTRAQ	http://www.securityfocus.com/bid/106423
BUGTRAQ	http://www.securityfocus.com/bid/106411
BUGTRAQ	http://www.securityfocus.com/bid/106436
BUGTRAQ	http://www.securityfocus.com/bid/106425
BUGTRAQ	http://www.securityfocus.com/bid/106437
BUGTRAQ	http://www.securityfocus.com/bid/106412
BUGTRAQ	http://www.securityfocus.com/bid/106421
BUGTRAQ	http://www.securityfocus.com/bid/106435
BUGTRAQ	http://www.securityfocus.com/bid/106386
BUGTRAQ	http://www.securityfocus.com/bid/106424
BUGTRAQ	http://www.securityfocus.com/bid/106385
BUGTRAQ	http://www.securityfocus.com/bid/106432
BUGTRAQ	http://www.securityfocus.com/bid/106433
BUGTRAQ	http://www.securityfocus.com/bid/106430
BUGTRAQ	http://www.securityfocus.com/bid/106407
BUGTRAQ	http://www.securityfocus.com/bid/106414
BUGTRAQ	http://www.securityfocus.com/bid/106431
BUGTRAQ	http://www.securityfocus.com/bid/106428
BUGTRAQ	http://www.securityfocus.com/bid/106395
BUGTRAQ	http://www.securityfocus.com/bid/106394

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/106419
BUGTRAQ	http://www.securityfocus.com/bid/106406
BUGTRAQ	http://www.securityfocus.com/bid/106429
BUGTRAQ	http://www.securityfocus.com/bid/106415
BUGTRAQ	http://www.securityfocus.com/bid/106400
BUGTRAQ	http://www.securityfocus.com/bid/106465
URL	https://support.microsoft.com/en-us/help/4480978
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001
URL	https://support.microsoft.com/en-us/help/3173424
URL	https://support.microsoft.com/en-us/help/4465659
URL	https://support.microsoft.com/en-us/help/4093430
URL	https://support.microsoft.com/en-us/help/3177467
URL	https://support.microsoft.com/en-us/help/3173426
URL	https://support.microsoft.com/en-us/help/4480968
URL	https://support.microsoft.com/en-us/help/4480966
URL	https://support.microsoft.com/en-us/help/4480961
URL	https://support.microsoft.com/en-us/help/4480973
URL	https://support.microsoft.com/en-us/help/4480970
URL	https://support.microsoft.com/en-us/help/4480116
URL	https://support.microsoft.com/en-us/help/4480963
URL	https://support.microsoft.com/en-us/help/4480962
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4486458

Type	Reference
URL	https://support.microsoft.com/en-us/help/4461624
URL	https://support.microsoft.com/en-us/help/4480972
URL	https://support.microsoft.com/en-us/help/4461591
URL	https://support.microsoft.com/en-us/help/4470788
URL	https://support.microsoft.com/en-us/help/4468742
URL	https://support.microsoft.com/en-us/help/4480957
URL	https://support.microsoft.com/en-us/help/4480964
URL	https://support.microsoft.com/en-us/help/4461634
URL	https://support.microsoft.com/en-us/help/4480960
URL	https://support.microsoft.com/en-us/help/955430
URL	https://support.microsoft.com/en-us/help/4477137
URL	https://support.microsoft.com/en-us/help/4471389
URL	https://support.microsoft.com/en-us/help/4477136
URL	https://support.microsoft.com/en-us/help/4476755
URL	https://support.microsoft.com/en-us/help/4461596
URL	https://support.microsoft.com/en-us/help/4476698
URL	https://support.microsoft.com/en-us/help/4461598
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0570
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0622
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0580
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0536
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0562

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0538
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0547
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0555
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0572
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0574
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0569
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0552
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0573
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0582
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0581
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0550
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0578
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0551
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0583

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0586
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0553
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0588
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0579
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0584
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0554
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0577
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0543
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0556
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0546
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0549
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0575
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0576
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0557
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0537
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0571

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0558
URL	https://support.microsoft.com/en-us/help/4480975

MS19-JUL: Microsoft Internet Explorer Security Update | High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-1056 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1059 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1063 - Internet Explorer Memory Corruption Vulnerability
CVE-2019-1104 - Microsoft Browser Memory Corruption Vulnerability
CVE-2019-1001 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1004 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Microsoft Edge on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems
ChakraCore

Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

Solution Details

Microsoft has released a fix for this flaw in their July 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1001
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1059
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1056
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1104
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1004

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1063
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1059
URL	https://support.microsoft.com/en-us/help/4507434
URL	https://support.microsoft.com/en-us/help/4507448
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1004
URL	https://support.microsoft.com/en-us/help/4507450
URL	https://support.microsoft.com/en-us/help/4507449
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1001
URL	https://support.microsoft.com/en-us/help/4507435
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1063
URL	https://support.microsoft.com/en-us/help/4507453
URL	https://support.microsoft.com/en-us/help/4507458
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1104
URL	https://support.microsoft.com/en-us/help/4507452
URL	https://support.microsoft.com/en-us/help/4507455
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1056
URL	https://support.microsoft.com/en-us/help/4507462
URL	https://support.microsoft.com/en-us/help/4507460
URL	https://support.microsoft.com/en-us/help/4507469

MS19-JUL: Microsoft SQL Server Security Update High

Solution Details

Microsoft has released a fix for this flaw in their July 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft SQL Server which include fixes for the following vulnerabilities:

CVE-2019-1068 - Microsoft SQL Server Remote Code Execution Vulnerability

Affected Products:
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (GDR)
Microsoft SQL Server 2017 for x64-based Systems (GDR)
Microsoft SQL Server 2014 Service Pack 2 for 32-bit Systems (CU+GDR)
Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems (CU+GDR)
Microsoft SQL Server 2017 for x64-based Systems (CU+GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (CU+GDR)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU+GDR)
Microsoft SQL Server 2014 Service Pack 2 for 32-bit Systems (GDR)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 1 (CU+GDR)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU+GDR)
Microsoft SQL Server 2014 Service Pack 2 for x64-based Systems (GDR)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.5

CVSS Vector: AV:N/AC:L/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1068
URL	https://support.microsoft.com/en-us/help/4505220
URL	https://support.microsoft.com/en-us/help/4505218
URL	https://support.microsoft.com/en-us/help/4505222
URL	https://support.microsoft.com/en-us/help/4505219
URL	https://support.microsoft.com/en-us/help/4505422

Type	Reference
URL	https://support.microsoft.com/en-us/help/4505225
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1068
URL	https://support.microsoft.com/en-us/help/4505217
URL	https://support.microsoft.com/en-us/help/4505221
URL	https://support.microsoft.com/en-us/help/4505419
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.microsoft.com/en-us/help/4505224

MS19-JUL: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-0865 - SymCrypt Denial of Service Vulnerability
CVE-2019-0887 - Remote Desktop ServicesÂ Remote Code Execution Vulnerability
CVE-2019-0966 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0975 - ADFS Security Feature Bypass Vulnerability
CVE-2019-1071 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-1072 - Azure DevOps Server and Team Foundation Server Remote Code Execution Vulnerability
CVE-2019-1073 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-1076 - Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-1093 - DirectWrite Information Disclosure Vulnerability
CVE-2019-1094 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1095 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1096 - Win32k Information Disclosure Vulnerability
CVE-2019-1097 - DirectWrite Information Disclosure Vulnerability
CVE-2019-1098 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1099 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1100 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1101 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1102 - GDI+ Remote Code Execution Vulnerability
CVE-2019-1116 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1117 - DirectWrite Remote Code Execution Vulnerability
CVE-2019-1118 - DirectWrite Remote Code Execution Vulnerability
CVE-2019-1119 - DirectWrite Remote Code Execution Vulnerability
CVE-2019-1120 - DirectWrite Remote Code Execution Vulnerability

CVE-2019-1121 - DirectWrite Remote Code Execution Vulnerability
CVE-2019-1122 - DirectWrite Remote Code Execution Vulnerability
CVE-2019-1123 - DirectWrite Remote Code Execution Vulnerability
CVE-2019-1124 - DirectWrite Remote Code Execution Vulnerability
CVE-2019-1126 - ADFS Security Feature Bypass Vulnerability
CVE-2019-1127 - DirectWrite Remote Code Execution Vulnerability
CVE-2019-1128 - DirectWrite Remote Code Execution Vulnerability
ADV990001 - Latest Servicing Stack Updates
CVE-2019-0785 - Windows DHCP Server Remote Code Execution Vulnerability
CVE-2019-0811 - Windows DNS Server Denial of Service Vulnerability
CVE-2019-0880 - Microsoft splwow64 Elevation of Privilege Vulnerability
CVE-2019-0962 - Azure Automation Elevation of Privilege Vulnerability
CVE-2019-0999 - DirectX Elevation of Privilege Vulnerability
CVE-2019-1037 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2019-1067 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1074 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1075 - ASP.NET Core Spoofing Vulnerability
CVE-2019-1077 - Visual Studio Elevation of Privilege Vulnerability
CVE-2019-1079 - Visual Studio Information Disclosure Vulnerability
CVE-2019-1082 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1085 - Windows WLAN Service Elevation of Privilege Vulnerability
CVE-2019-1086 - Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1087 - Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1088 - Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1089 - Windows RPCSS Elevation of Privilege Vulnerability
CVE-2019-1090 - Windows dnsrlvr.dll Elevation of Privilege Vulnerability
CVE-2019-1091 - Microsoft unistore.dll Information Disclosure Vulnerability
CVE-2019-1108 - Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2019-1129 - Windows Elevation of Privilege Vulnerability
CVE-2019-1130 - Windows Elevation of Privilege Vulnerability
CVE-2019-1132 - Win32k Elevation of Privilege Vulnerability

Affected Products:
ASP.NET Core 2.1
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.1
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Azure Automation
Microsoft Visual Studio 2013 Update 5
Windows Server 2012
Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
ASP.NET Core 2.2
Windows 7 for x64-based Systems Service Pack 1

Windows 10 Version 1803 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Microsoft Visual Studio 2017 version 15.9
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Microsoft Visual Studio 2012 Update 5
Windows 8.1 for 32-bit systems
Team Foundation Server 2012 Update 4
Team Foundation Server 2017 Update 3.1
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1903 for 32-bit Systems
Team Foundation Server 2010 SP1 (x86)
Team Foundation Server 2018 Update 3.2
Windows 10 Version 1803 for 32-bit Systems
Team Foundation Server 2013 Update 5
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Azure DevOps Server 2019.0.1
Microsoft Visual Studio 2010 Service Pack 1
Microsoft Visual Studio 2015 Update 3
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1703 for 32-bit Systems
Team Foundation Server 2018 Update 1.2
Windows 10 Version 1803 for ARM64-based Systems
Team Foundation Server 2010 SP1 (x64)
Windows 10 Version 1903 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Team Foundation Server 2015 Update 4.2
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Solution Details

Microsoft has released a fix for this flaw in their July 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0880
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1102
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0975
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0785
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1071
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1108
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1074
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0887
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1124
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1091
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1123
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1072
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0999
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1116
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1098
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1067
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1082
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1122
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1090
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1079
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1100

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1097
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1127
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1101
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1099
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0865
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1095
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1076
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1094
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1119
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1075
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0811
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1128
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1077
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1096
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1087
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0966
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1073
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1132
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0962
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1089
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1093
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1120
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1086
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1117

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1121
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1118
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1126
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1130
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1037
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1129
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1085
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1088
URL	https://support.microsoft.com/en-us/help/4509090
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1121
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1117
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1126
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1130
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1085
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0966
URL	https://cwe.mitre.org/data/definitions/601.html
URL	http://packetstormsecurity.com/files/153683/Microsoft-Windows-RPCSS-Activation-Kernel-Security-Callback-Privilege-Escalation.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://cwe.mitre.org/data/definitions/254.html

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1129
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1037
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1120
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1093
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1132
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1096
URL	https://support.microsoft.com/en-us/help/4507457
URL	https://support.microsoft.com/en-us/help/4509092
URL	https://support.microsoft.com/en-us/help/4509091
URL	https://support.microsoft.com/en-us/help/4507456
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0999
URL	https://support.microsoft.com/en-us/help/4509093
URL	https://support.microsoft.com/en-us/help/4504418
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1116
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1098
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1067
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1082

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1122
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1090
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1079
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1100
URL	https://support.microsoft.com/en-us/help/4506162
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1101
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1099
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0865
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1095
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1076
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1097
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1094
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1119
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1075
URL	https://support.microsoft.com/en-us/help/4490628
URL	https://support.microsoft.com/en-us/help/4493730
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001

Type	Reference
URL	https://support.microsoft.com/en-us/help/4507455
URL	https://support.microsoft.com/en-us/help/4507460
URL	https://support.microsoft.com/en-us/help/4507449
URL	https://support.microsoft.com/en-us/help/4507469
URL	https://support.microsoft.com/en-us/help/4507462
URL	https://support.microsoft.com/en-us/help/4507450
URL	https://support.microsoft.com/en-us/help/4507448
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1086
URL	https://support.microsoft.com/en-us/help/4507453
URL	https://support.microsoft.com/en-us/help/4507458
URL	https://support.microsoft.com/en-us/help/4507452
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1089
URL	https://support.microsoft.com/en-us/help/4507435
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1091
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1124
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0887
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1074
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1088
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0880
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1102

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0975
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0785
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1071
URL	https://support.microsoft.com/en-us/help/4509095
URL	https://support.microsoft.com/en-us/help/4509094
URL	https://support.microsoft.com/en-us/help/4506163
URL	https://support.microsoft.com/en-us/help/4509096
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1108
URL	https://support.microsoft.com/en-us/help/4506161
URL	https://support.microsoft.com/en-us/help/4507461
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1123
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0962
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1073
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1072
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0811
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1128
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1077

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1087
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1127
URL	https://support.microsoft.com/en-us/help/4506164
URL	https://support.microsoft.com/en-us/help/4507464
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1118

MS19-JUN: Microsoft Internet Explorer Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-0988 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1055 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-0920 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1005 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1038 - Microsoft Browser Memory Corruption Vulnerability
CVE-2019-1080 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1081 - Microsoft Browser Information Disclosure Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems

Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Microsoft Edge on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their June 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1080

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1081
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1055
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0920
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0988
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1038
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1005
URL	https://support.microsoft.com/en-us/help/4503273
URL	https://support.microsoft.com/en-us/help/4503285
URL	https://support.microsoft.com/en-us/help/4503279
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-639/
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-638/
URL	https://support.microsoft.com/en-us/help/4503292
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-627/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1038
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1081
URL	https://support.microsoft.com/en-us/help/4503276
URL	https://support.microsoft.com/en-us/help/4503287
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0920
URL	https://support.microsoft.com/en-us/help/4503290
URL	https://support.microsoft.com/en-us/help/4503259
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1080

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0988
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1005
URL	https://support.microsoft.com/en-us/help/4503293
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1055
URL	https://support.microsoft.com/en-us/help/4503327
URL	https://support.microsoft.com/en-us/help/4503291
URL	https://support.microsoft.com/en-us/help/4503286
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-626/
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-625/
URL	https://support.microsoft.com/en-us/help/4503267
URL	https://support.microsoft.com/en-us/help/4503284

MS19-JUN: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-0888 - ActiveX Data Objects (ADO) Remote Code Execution Vulnerability
CVE-2019-0904 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0905 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0906 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0907 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0908 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0909 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0941 - Microsoft IIS Server Denial of Service Vulnerability
CVE-2019-0943 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2019-0948 - Windows Event Viewer Information Disclosure Vulnerability
CVE-2019-0959 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2019-0972 - Local Security Authority Subsystem Service Denial of Service Vulnerability
CVE-2019-0973 - Windows Installer Elevation of Privilege Vulnerability

CVE-2019-0974 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0984 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2019-1009 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1010 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1011 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1012 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1013 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1014 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1015 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1016 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1017 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1018 - DirectX Elevation of Privilege Vulnerability
CVE-2019-1029 - Skype for Business and Lync Server Denial of Service Vulnerability
CVE-2019-1046 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1047 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1048 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1049 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1050 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0620 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-0709 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-0710 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0711 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0713 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0722 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-0960 - Win32k Elevation of Privilege Vulnerability
CVE-2019-0968 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0977 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0983 - Windows Storage Service Elevation of Privilege Vulnerability
CVE-2019-0985 - Microsoft Speech API Remote Code Execution Vulnerability
CVE-2019-0986 - Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2019-0996 - Azure DevOps Server Spoofing Vulnerability
CVE-2019-0998 - Windows Storage Service Elevation of Privilege Vulnerability
CVE-2019-1007 - Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1019 - Microsoft Windows Security Feature Bypass Vulnerability
CVE-2019-1021 - Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1022 - Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1025 - Windows Denial of Service Vulnerability
CVE-2019-1026 - Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1027 - Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1028 - Windows Audio Service Elevation of Privilege Vulnerability

Solution Details

Microsoft has released a fix for this flaw in their June 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0983
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1047
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1053
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0977
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1039
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0972
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1065
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1029
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0973
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1064
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1019
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0906
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1050
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0709
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1045
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0998
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1014
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1046
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1048
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1069
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1011
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0985
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1027

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1021
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0960
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1013
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0959
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1007
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1012
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0941
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0984
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1018
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1016
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1009
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0905
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1025
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0909
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0722
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0974
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0996
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1022
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1017
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0943
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1040
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0711
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0907
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1015

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1041
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0713
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1028
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0620
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1044
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0986
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0888
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0904
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0710
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1010
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0968
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1026
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1049
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0908
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0948
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1043
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1009
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1016
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1018
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0984
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0941

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1012
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1007
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0959
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1013
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-580/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0960
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1021
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1027
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0985
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-573/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1011
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1069
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1048
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1046
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1014

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0998
URL	https://support.microsoft.com/en-us/help/4493730
URL	https://support.microsoft.com/en-us/help/4500109
URL	https://support.microsoft.com/en-us/help/4504369
URL	https://support.microsoft.com/en-us/help/4503290
URL	https://support.microsoft.com/en-us/help/4506009
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-641/
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-624/
URL	https://support.microsoft.com/en-us/help/4503263
URL	https://support.microsoft.com/en-us/help/4503269
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1041
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1015
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0943
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1017
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0974
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0909
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1045
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0906
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1019

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1064
URL	https://support.microsoft.com/en-us/help/4503287
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190017
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0973
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1029
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0948
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0986
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0888
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0904
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0710
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0908
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1049
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1010
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0968
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1026
URL	https://cwe.mitre.org/data/definitions/19.html

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.microsoft.com/en-us/help/4490628
URL	https://support.microsoft.com/en-us/help/3173424
URL	https://cwe.mitre.org/data/definitions/352.html
URL	https://support.microsoft.com/en-us/help/4503292
URL	https://support.microsoft.com/en-us/help/3173426
URL	https://support.microsoft.com/en-us/help/4500641
URL	https://support.microsoft.com/en-us/help/4500640
URL	https://support.microsoft.com/en-us/help/4497398
URL	https://support.microsoft.com/en-us/help/4498353
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0709
URL	https://support.microsoft.com/en-us/help/4503537
URL	http://packetstormsecurity.com/files/153639/Microsoft-Windows-HTTP-To-SMB-NTLM-Reflection-Privilege-Escalation.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://support.microsoft.com/en-us/help/4503285
URL	https://support.microsoft.com/en-us/help/4503279
URL	https://support.microsoft.com/en-us/help/4503286
URL	https://support.microsoft.com/en-us/help/4503276
URL	https://support.microsoft.com/en-us/help/4503273
URL	https://support.microsoft.com/en-us/help/4503267
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-571/
URL	https://blog.0patch.com/2019/06/another-task-scheduler-0day-another.html

Type	Reference
URL	https://support.microsoft.com/en-us/help/4503291
URL	https://support.microsoft.com/en-us/help/4503293
URL	https://support.microsoft.com/en-us/help/4503284
URL	https://support.microsoft.com/en-us/help/4503327
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0905
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0907
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0713
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1028
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0620
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1044
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1065
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190016
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0972
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0722
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1039
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0977
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1053

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1047
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0711
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0983
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1050
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1043
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1025
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0996
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1022
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1040

MS19-MAR: Microsoft Internet Explorer Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their March 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-0609 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-0746 - Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2019-0761 - Internet Explorer Security Feature Bypass Vulnerability
CVE-2019-0762 - Microsoft Browsers Security Feature Bypass Vulnerability

CVE-2019-0763 - Internet Explorer Memory Corruption Vulnerability
CVE-2019-0768 - Internet Explorer Security Feature Bypass Vulnerability
CVE-2019-0780 - Microsoft Browser Memory Corruption Vulnerability
CVE-2019-0783 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-0665 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2019-0666 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2019-0667 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2019-0680 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Microsoft Edge on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems

Microsoft Edge on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0665
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0609
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0761
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0680
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0667
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0763
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0762
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0746
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0666
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0780
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0783
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0768
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0665
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0609
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0761

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0762
URL	https://support.microsoft.com/en-us/help/4489880
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0780
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0666
URL	https://support.microsoft.com/en-us/help/4489868
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0763
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0746
URL	https://support.microsoft.com/en-us/help/4489882
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0667
URL	https://support.microsoft.com/en-us/help/4489872
URL	https://support.microsoft.com/en-us/help/4489873
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0680
URL	https://support.microsoft.com/en-us/help/4489886
URL	https://support.microsoft.com/en-us/help/4489871
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0783
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0768
URL	https://support.microsoft.com/en-us/help/4489878
URL	https://support.microsoft.com/en-us/help/4489891
URL	https://support.microsoft.com/en-us/help/4489899

Type	Reference
URL	https://support.microsoft.com/en-us/help/4489881

MS19-MAR: Microsoft Windows Security Update

High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-0754 - Windows Denial of Service Vulnerability
CVE-2019-0755 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0756 - MS XML Remote Code Execution Vulnerability
CVE-2019-0759 - Windows Print Spooler Information Disclosure Vulnerability
CVE-2019-0765 - Comctl32 Remote Code Execution Vulnerability
CVE-2019-0766 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-0767 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0772 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2019-0774 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0775 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0776 - Win32k Information Disclosure Vulnerability
CVE-2019-0777 - Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-0778 - Microsoft Office SharePoint XSS Vulnerability
CVE-2019-0782 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0784 - Windows ActiveX Remote Code Execution Vulnerability
CVE-2019-0797 - Win32k Elevation of Privilege Vulnerability
ADV190009 - SHA-2 Code Sign Support Advisory
CVE-2019-0798 - Skype for Business and Lync Spoofing Vulnerability
ADV190010 - Best Practices Regarding Sharing of a Single User Account Across Multiple Users
CVE-2019-0808 - Win32k Elevation of Privilege Vulnerability
CVE-2019-0816 - Azure SSH Keypairs Security Feature Bypass Vulnerability
ADV990001 - Latest Servicing Stack Updates
CVE-2019-0603 - Windows Deployment Services TFTP Server Remote Code Execution Vulnerability
CVE-2019-0614 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0617 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0682 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0683 - Active Directory Elevation of Privilege Vulnerability
CVE-2019-0689 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0690 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0692 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0693 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0694 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-0695 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0696 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-0697 - Windows DHCP Client Remote Code Execution Vulnerability
CVE-2019-0698 - Windows DHCP Client Remote Code Execution Vulnerability
CVE-2019-0701 - Windows Hyper-V Denial of Service Vulnerability

CVE-2019-0702 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-0703 - Windows SMB Information Disclosure Vulnerability
CVE-2019-0704 - Windows SMB Information Disclosure Vulnerability
CVE-2019-0726 - Windows DHCP Client Remote Code Execution Vulnerability
CVE-2019-0809 - Visual Studio Remote Code Execution Vulnerability
CVE-2019-0821 - Windows SMB Information Disclosure Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Lync Server 2013 July 2018 Update
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Team Foundation Server 2018 Updated 1.2
UbuntuServer:18.04-LTS
Team Foundation Server 2017 Update 3.1
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Team Foundation Server 2018 Update 3.2
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Skype for Business Server 2015 March 2019 Update
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft SharePoint Foundation 2013 Service Pack 1

Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
None Available
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their March 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0765
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0755
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0777
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0776
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0754
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0782
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0689
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0695
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0617
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0726
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0774
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0614
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0797
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0692

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0698
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0766
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0772
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0756
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0821
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0696
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0775
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0693
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0809
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0798
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0816
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0682
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0694
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0767
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0603
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0683
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0690
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0704
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0759
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0778
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0784
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0703
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0702
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0808

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0701
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0697
URL	https://support.microsoft.com/en-us/help/4485449
URL	https://support.microsoft.com/en-us/help/4489885
URL	https://support.microsoft.com/en-us/help/4485448
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/3061064
URL	https://support.microsoft.com/en-us/help/4489883
URL	https://support.microsoft.com/en-us/help/4462208
URL	https://support.microsoft.com/en-us/help/4485447
URL	https://support.microsoft.com/en-us/help/4489884
URL	https://support.microsoft.com/en-us/help/4491476
URL	https://support.microsoft.com/en-us/help/2809243
URL	https://support.microsoft.com/en-us/help/4462211
URL	https://cwe.mitre.org/data/definitions/426.html
URL	https://cwe.mitre.org/data/definitions/611.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/190.html
URL	http://packetstormsecurity.com/files/153407/Microsoft-Windows-CmpAddRemoveContainerToCLFSLog-Arbitrary-File-Directory-Creation.html
URL	http://packetstormsecurity.com/files/153408/Microsoft-Windows-Font-Cache-Service-Insecure-Sections.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://support.microsoft.com/en-us/help/955430

Type	Reference
URL	https://support.microsoft.com/en-us/help/4470788
URL	https://support.microsoft.com/en-us/help/4489878
URL	https://support.microsoft.com/en-us/help/4489891
URL	https://support.microsoft.com/en-us/help/4489899
URL	https://support.microsoft.com/en-us/help/4489882
URL	https://support.microsoft.com/en-us/help/4489868
URL	https://support.microsoft.com/en-us/help/4489880
URL	https://support.microsoft.com/en-us/help/4489872
URL	https://support.microsoft.com/en-us/help/4489886
URL	https://support.microsoft.com/en-us/help/4489871
URL	https://support.microsoft.com/en-us/help/4489881
URL	https://support.microsoft.com/en-us/help/3173426
URL	https://support.microsoft.com/en-us/help/4093430
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0755
URL	https://support.microsoft.com/en-us/help/3173424
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0777
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0776
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0754
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0782
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0689

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0695
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0617
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0726
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0614
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190009
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0797
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0692
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0766
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0772
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0756
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0696
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0775
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0821
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0698
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190010
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0774

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0765
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0697
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0701
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0808
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0702
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0703
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0784
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0778
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0759
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0704
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0690
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0683
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0603
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0767
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0694

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0682
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0816
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0798
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0809
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0693
URL	https://support.microsoft.com/en-us/help/4490628
URL	https://support.microsoft.com/en-us/help/4487327
URL	https://support.microsoft.com/en-us/help/4474419
URL	https://support.microsoft.com/en-us/help/4489876

MS19-MAY: Microsoft Internet Explorer Security Update High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-0884 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-0911 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-0918 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-0921 - Internet Explorer Spoofing Vulnerability
CVE-2019-0929 - Internet Explorer Memory Corruption Vulnerability
CVE-2019-0930 - Internet Explorer Information Disclosure Vulnerability
CVE-2019-0940 - Microsoft Browser Memory Corruption Vulnerability
CVE-2019-0995 - Internet Explorer Security Feature Bypass Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems

Microsoft Edge on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge on Windows Server 2016
Microsoft Edge on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Microsoft Edge on Windows 10 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge on Windows 10 Version 1903 for 32-bit Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Microsoft Edge on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems

Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2012
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

Solution Details

Microsoft has released a fix for this flaw in their May 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0884
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0918
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0995
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0940
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0921
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0930
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0929
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0911
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0929
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4499171
URL	https://support.microsoft.com/en-us/help/4499154
URL	https://support.microsoft.com/en-us/help/4499164
URL	https://support.microsoft.com/en-us/help/4499167
URL	https://support.microsoft.com/en-us/help/4499149

Type	Reference
URL	https://support.microsoft.com/en-us/help/4494440
URL	https://support.microsoft.com/en-us/help/4499181
URL	https://support.microsoft.com/en-us/help/4499151
URL	https://support.microsoft.com/en-us/help/4494441
URL	https://support.microsoft.com/en-us/help/4497936
URL	https://support.microsoft.com/en-us/help/4499179
URL	https://support.microsoft.com/en-us/help/4498206
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0884
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0918
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0995
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0940
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0921
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0930
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0911

MS19-MAY: Microsoft Windows Security Update (ZombieLoad) High

Solution Details

Microsoft has released a fix for this flaw in their May 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-0863 - Windows Error Reporting Elevation of Privilege Vulnerability

CVE-2019-0882 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0886 - Windows Hyper-V Information Disclosure Vulnerability
CVE-2019-0892 - Win32k Elevation of Privilege Vulnerability
CVE-2019-0893 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0894 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0895 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0896 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0897 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0898 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0899 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0900 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0901 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0902 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0903 - GDI+ Remote Code Execution Vulnerability
CVE-2019-0932 - Skype for Android Information Disclosure Vulnerability
CVE-2019-0942 - Unified Write Filter Elevation of Privilege Vulnerability
CVE-2019-0956 - Microsoft SharePoint Server Information Disclosure Vulnerability
CVE-2019-0957 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2019-0958 - Microsoft SharePoint Elevation of Privilege Vulnerability
CVE-2019-0961 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0963 - Microsoft Office SharePoint XSS Vulnerability
CVE-2019-0971 - Azure DevOps Server and Team Foundation Server Information Disclosure Vulnerability
CVE-2019-0982 - ASP.NET Core Denial of Service Vulnerability
ADV990001 - Latest Servicing Stack Updates
CVE-2019-0707 - Windows NDIS Elevation of Privilege Vulnerability
CVE-2019-0708 - Remote Desktop ServicesÂ Remote Code Execution Vulnerability
CVE-2019-0725 - Windows DHCP Server Remote Code Execution Vulnerability
CVE-2019-0727 - Diagnostic Hub Standard Collector, Visual Studio Standard Collector Elevation of Privilege Vulnerability
CVE-2019-0733 - Windows Defender Application Control Security Feature Bypass Vulnerability
CVE-2019-0734 - Windows Elevation of Privilege Vulnerability
CVE-2019-0758 - Windows GDI Information Disclosure Vulnerability
CVE-2019-0872 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-0881 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-0885 - Windows OLE Remote Code Execution Vulnerability
CVE-2019-0889 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0890 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0891 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-0931 - Windows Storage Service Elevation of Privilege Vulnerability
ADV190013 - Microsoft Guidance to mitigate Microarchitectural Data Sampling vulnerabilities
CVE-2019-0936 - Windows Elevation of Privilege Vulnerability
CVE-2019-0949 - Microsoft SharePoint Spoofing Vulnerability
CVE-2019-0950 - Microsoft SharePoint Spoofing Vulnerability
CVE-2019-0951 - Microsoft SharePoint Spoofing Vulnerability
CVE-2019-0952 - Microsoft SharePoint Server Remote Code Execution Vulnerability
CVE-2019-0976 - NuGet Package Manager Tampering Vulnerability
CVE-2019-0979 - Azure DevOps Server and Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-1000 - Microsoft Azure AD Connect Elevation of Privilege Vulnerability

CVE-2019-1008 - Microsoft Dynamics On-Premise Security Feature Bypass

Affected Products:
ASP.NET Core 2.1
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Microsoft Visual Studio 2019 version 16.0
ASP.NET Core 2.2
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Nuget 5.0.2
Windows 10 Version 1703 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Microsoft Dynamics CRM 2015 (on-premises) version 7.0
Team Foundation Server 2017 Update 3.1
Windows 10 Version 1903 for 32-bit Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft Dynamics 365 (on-premises) version 9.0
Team Foundation Server 2018 Update 3.2
Windows 10 Version 1803 for 32-bit Systems
Microsoft Dynamics 365 (on-premises) version 8.2
Azure DevOps Server 2019
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Microsoft SharePoint Foundation 2010 Service Pack 2
Microsoft Visual Studio 2015 Update 3

Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Team Foundation Server 2018 Update 1.2
Microsoft SharePoint Foundation 2013 Service Pack 1
Windows 10 Version 1803 for ARM64-based Systems
Skype 8.35 when installed on Android Devices
Windows 10 Version 1903 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Team Foundation Server 2015 Update 4.2
Microsoft Visual Studio 2017 version 15.0
Windows Server 2016
Microsoft Azure Active Directory Connect
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft SharePoint Server 2019
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0886
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0863
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0932
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0892
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0958
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0708
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0707
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0894
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0942
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0897
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0976

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0758
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0956
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0896
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0890
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0733
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0872
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0957
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0979
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12126
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12127
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-11091
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12130
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0881
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0893
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0950
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0727
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0899
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0952
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0891
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0889
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0885
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0951
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1008
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0900

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0725
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0971
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0903
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0949
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0963
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0936
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1000
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0902
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0734
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0982
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0882
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0901
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0961
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0898
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0895
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0931
BUGTRAQ	http://www.securityfocus.com/bid/108210
URL	https://support.microsoft.com/en-us/help/4490628
URL	https://support.microsoft.com/en-us/help/4499179
URL	https://support.microsoft.com/en-us/help/4497936
URL	https://support.microsoft.com/en-us/help/4494441
URL	https://support.microsoft.com/en-us/help/4499151
URL	https://support.microsoft.com/en-us/help/4499181
URL	https://support.microsoft.com/en-us/help/4494440

Type	Reference
URL	https://support.microsoft.com/en-us/help/4499149
URL	https://support.microsoft.com/en-us/help/4499167
URL	https://support.microsoft.com/en-us/help/4499164
URL	https://support.microsoft.com/en-us/help/4499154
URL	https://support.microsoft.com/en-us/help/4499171
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0950
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0727
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0899
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0952
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0891
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0889
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0885
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0951
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1008
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0900
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0725
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0971

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0903
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0949
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0963
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0936
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1000
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0902
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0734
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0982
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0882
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190013
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0901
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0961
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0898
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0895
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0893

Type	Reference
URL	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20190529-01-windows-en
URL	http://www.huawei.com/en/psirt/security-notices/huawei-sn-20190515-01-windows-en
URL	http://packetstormsecurity.com/files/153133/Microsoft-Windows-Remote-Desktop-BlueKeep-Denial-Of-Service.html
URL	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	http://packetstormsecurity.com/files/152988/Microsoft-Windows-CmKeyBodyRemapToVirtualForEnum-Arbitrary-Key-Enumeration.html
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-932041.pdf
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-832947.pdf
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-616199.pdf
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-433987.pdf
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-406175.pdf
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-166360.pdf
URL	http://packetstormsecurity.com/files/153008/Angry-Polar-Bear-2-Microsoft-Windows-Error-Reporting-Local-Privilege-Escalation.html
URL	https://support.microsoft.com/en-us/help/3173424
URL	https://support.microsoft.com/en-us/help/3173426
URL	https://support.microsoft.com/en-us/help/4493730
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0931

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0886
URL	http://packetstormsecurity.com/files/153627/Microsoft-Windows-RDP-BlueKeep-Denial-Of-Service.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0863
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0932
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0892
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0958
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0707
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0894
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0942
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0897
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0976
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0758
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0956

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0896
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0890
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0733
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0872
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0881
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0957
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0979
URL	https://support.microsoft.com/en-us/help/4489639
URL	https://support.microsoft.com/en-us/help/4500641
URL	https://support.microsoft.com/en-us/help/4498363
URL	https://support.microsoft.com/en-us/help/4499158
URL	https://support.microsoft.com/en-us/help/4499728
URL	https://support.microsoft.com/en-us/help/4464549
URL	https://support.microsoft.com/en-us/help/4464556
URL	https://support.microsoft.com/en-us/help/4500640
URL	https://support.microsoft.com/en-us/help/4497398
URL	https://support.microsoft.com/en-us/help/4498353
URL	https://support.microsoft.com/en-us/help/4499175
URL	https://support.microsoft.com/en-us/help/4464573
URL	https://support.microsoft.com/en-us/help/4464564
URL	https://support.microsoft.com/en-us/help/4499165

Type	Reference
URL	https://support.microsoft.com/en-us/help/4498947
URL	https://support.microsoft.com/en-us/help/4499180
URL	https://support.microsoft.com/en-us/help/4499386
URL	https://support.microsoft.com/en-us/help/4494412

MS19-NOV: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their November 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-1429 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1390 - VBScript Remote Code Execution Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems

Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2012
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1429
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1390
URL	https://support.microsoft.com/en-us/help/4525237
URL	https://support.microsoft.com/en-us/help/4524570
URL	https://support.microsoft.com/en-us/help/4525106
URL	https://support.microsoft.com/en-us/help/4525234
URL	https://support.microsoft.com/en-us/help/4525232
URL	https://support.microsoft.com/en-us/help/4525243
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1390
URL	https://support.microsoft.com/en-us/help/4525236
URL	https://support.microsoft.com/en-us/help/4525241
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1429
URL	https://support.microsoft.com/en-us/help/4525246
URL	https://support.microsoft.com/en-us/help/4525235
URL	https://support.microsoft.com/en-us/help/4523205

MS19-NOV: Microsoft Windows Security Update High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their November 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-1234 - Azure Stack Spoofing Vulnerability
CVE-2019-1374 - Windows Error Reporting Information Disclosure Vulnerability
CVE-2019-1415 - Windows Installer Elevation of Privilege Vulnerability
CVE-2019-1416 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2019-1417 - Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2019-1418 - Windows Modules Installer Service Information Disclosure Vulnerability
CVE-2019-1430 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2019-1432 - DirectWrite Information Disclosure Vulnerability
CVE-2019-1433 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2019-1434 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1435 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2019-1436 - Win32k Information Disclosure Vulnerability
CVE-2019-1437 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2019-1438 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2019-1439 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1440 - Win32k Information Disclosure Vulnerability
CVE-2019-1441 - Win32k Graphics Remote Code Execution Vulnerability
CVE-2019-11135 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-1456 - OpenType Font Parsing Remote Code Execution Vulnerability
CVE-2018-12207 - Windows Denial of Service Vulnerability
ADV190024 - Microsoft Guidance for Vulnerability in Trusted Platform Module (TPM)
ADV990001 - Latest Servicing Stack Updates
CVE-2019-0712 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-0719 - Hyper-V Remote Code Execution Vulnerability
CVE-2019-0721 - Hyper-V Remote Code Execution Vulnerability
CVE-2019-1309 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-1310 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-1324 - Windows TCP/IP Information Disclosure Vulnerability
CVE-2019-1370 - Open Enclave SDK Information Disclosure Vulnerability
CVE-2019-1379 - Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2019-1380 - Microsoft splwow64 Elevation of Privilege Vulnerability
CVE-2019-1381 - Microsoft Windows Information Disclosure Vulnerability
CVE-2019-1382 - Microsoft ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2019-1383 - Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2019-1384 - Microsoft Windows Security Feature Bypass Vulnerability

CVE-2019-1385 - Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
CVE-2019-1388 - Windows Certificate Dialog Elevation of Privilege Vulnerability
CVE-2019-1389 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-1391 - Windows Denial of Service Vulnerability
CVE-2019-1392 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2019-1393 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1394 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1395 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1396 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1397 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-1398 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2019-1399 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-1405 - Windows UPnP Service Elevation of Privilege Vulnerability
CVE-2019-1406 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1407 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2019-1408 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1409 - Windows Remote Procedure Call Information Disclosure Vulnerability
CVE-2019-1411 - DirectWrite Information Disclosure Vulnerability
CVE-2019-1412 - OpenType Font Driver Information Disclosure Vulnerability
CVE-2019-1419 - OpenType Font Parsing Remote Code Execution Vulnerability
CVE-2019-1420 - Windows Elevation of Privilege Vulnerability
CVE-2019-1422 - Windows Elevation of Privilege Vulnerability
CVE-2019-1423 - Windows Elevation of Privilege Vulnerability
CVE-2019-1424 - NetLogon Security Feature Bypass Vulnerability
CVE-2019-1425 - Visual Studio Elevation of Privilege Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.3
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
Open Enclave SDK
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Azure Stack
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Microsoft Visual Studio 2017 version 15.9
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems

Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1903 for ARM64-based Systems
None affected
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

CVSS Base Score: 9.9

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1393
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0719
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1412
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12207
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1411
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1384
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1382
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1416
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1425
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1456

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1406
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1441
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1434
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1417
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1391
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1310
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1423
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1422
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1396
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1395
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1399
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1418
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1370
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1374
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1439
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1309
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1419
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1392
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1405
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1436
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1380
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1409
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1440
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1389

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1420
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1234
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1385
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1398
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1383
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1324
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1415
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0712
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1381
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1379
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0721
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1407
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1388
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1394
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1408
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1397
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1435
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1433
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1424
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1430
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1437
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1438
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1432
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-11135

Type	Reference
URL	https://support.microsoft.com/en-us/help/4526478
URL	https://support.microsoft.com/en-us/help/4520724
URL	https://support.microsoft.com/en-us/help/4525253
URL	https://support.microsoft.com/en-us/help/4525233
URL	https://support.microsoft.com/en-us/help/4523208
URL	https://support.microsoft.com/en-us/help/4521861
URL	https://support.microsoft.com/en-us/help/4521862
URL	https://support.microsoft.com/en-us/help/4521863
URL	https://support.microsoft.com/en-us/help/4521858
URL	https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0912
URL	https://support.microsoft.com/en-us/help/4525243
URL	https://support.microsoft.com/en-us/help/4525234
URL	https://support.microsoft.com/en-us/help/4524445
URL	https://support.microsoft.com/en-us/help/4525250
URL	https://support.microsoft.com/en-us/help/4523203
URL	https://support.microsoft.com/en-us/help/4523204
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1412
URL	https://support.microsoft.com/en-us/help/4524570
URL	https://support.microsoft.com/en-us/help/4525241
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-12207
URL	https://support.microsoft.com/en-us/help/4525236
URL	https://support.microsoft.com/en-us/help/4525232
URL	https://support.microsoft.com/en-us/help/4525246

Type	Reference
URL	https://support.microsoft.com/en-us/help/4525235
URL	https://support.microsoft.com/en-us/help/4523205
URL	https://support.microsoft.com/en-us/help/4525237
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1389
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1440
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1409
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1380
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190024
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1436
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1405
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1411
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1392
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1309
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1439
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1374
URL	https://support.microsoft.com/en-us/help/4523200
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1382

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1370
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1423
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1395
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1441
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1406
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1425
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1396
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1456
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1379
URL	https://support.microsoft.com/en-us/help/4523206
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1416
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1384
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-11135
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1430
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1424
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1397

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1408
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1394
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1388
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1407
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0721
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0712
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1415
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1324
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1383
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1398
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1437
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1438
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1432
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1393
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0719
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1433

Type	Reference
URL	https://support.microsoft.com/en-us/help/4523202
URL	https://support.microsoft.com/en-us/help/4524569
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1435
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1381
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1419
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1391
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1434
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1417
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1310
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1422
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1399
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1418
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1385
URL	https://support.microsoft.com/en-us/help/4525239
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1234
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1420
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001

MS19-OCT: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their October 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-0608 - Microsoft Browser Spoofing Vulnerability
CVE-2019-1371 - Internet Explorer Memory Corruption Vulnerability
CVE-2019-1238 - VBScript Remote Code Execution Vulnerability
CVE-2019-1239 - VBScript Remote Code Execution Vulnerability
CVE-2019-1357 - Microsoft Browser Spoofing Vulnerability

Affected Products:
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

Internet Explorer 10 on Windows Server 2012
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2012
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1357
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0608
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1238
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1371
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1239
URL	https://support.microsoft.com/en-us/help/4520010
URL	https://support.microsoft.com/en-us/help/4517389
URL	https://support.microsoft.com/en-us/help/4520002
URL	https://support.microsoft.com/en-us/help/4520004

Type	Reference
URL	https://support.microsoft.com/en-us/help/4520008
URL	https://support.microsoft.com/en-us/help/4519974
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0608
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1238
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1371
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1239
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1357
URL	https://support.microsoft.com/en-us/help/4520011
URL	https://support.microsoft.com/en-us/help/4520005
URL	https://support.microsoft.com/en-us/help/4520007
URL	https://support.microsoft.com/en-us/help/4519976
URL	https://support.microsoft.com/en-us/help/4519338
URL	https://support.microsoft.com/en-us/help/4519998

MS19-OCT: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their October 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-1060 - MS XML Remote Code Execution Vulnerability

CVE-2019-1341 - Windows Power Service Elevation of Privilege Vulnerability
CVE-2019-1342 - Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2019-1343 - Windows Denial of Service Vulnerability
CVE-2019-1344 - Windows Code Integrity Module Information Disclosure Vulnerability
CVE-2019-1345 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-1346 - Windows Denial of Service Vulnerability
CVE-2019-1347 - Windows Denial of Service Vulnerability
CVE-2019-1375 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
ADV990001 - Latest Servicing Stack Updates
CVE-2019-1166 - Windows NTLM Tampering Vulnerability
CVE-2019-1230 - Hyper-V Information Disclosure Vulnerability
CVE-2019-1311 - Windows Imaging API Remote Code Execution Vulnerability
CVE-2019-1313 - SQL Server Management Studio Information Disclosure Vulnerability
CVE-2019-1314 - Windows 10 Mobile Security Feature Bypass Vulnerability
CVE-2019-1315 - Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2019-1316 - Microsoft Windows Setup Elevation of Privilege Vulnerability
CVE-2019-1317 - Microsoft Windows Denial of Service Vulnerability
CVE-2019-1318 - Microsoft Windows Transport Layer Security Spoofing Vulnerability
CVE-2019-1319 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2019-1320 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1321 - Microsoft Windows CloudStore Elevation of Privilege Vulnerability
CVE-2019-1322 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1323 - Microsoft Windows Update Client Elevation of Privilege Vulnerability
CVE-2019-1325 - Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability
CVE-2019-1326 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2019-1333 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2019-1334 - Windows Kernel Information Disclosure Vulnerability
CVE-2019-1336 - Microsoft Windows Update Client Elevation of Privilege Vulnerability
CVE-2019-1337 - Windows Update Client Information Disclosure Vulnerability
CVE-2019-1338 - Windows NTLM Security Feature Bypass Vulnerability
CVE-2019-1339 - Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2019-1340 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2019-1358 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1359 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1361 - Microsoft Graphics Components Information Disclosure Vulnerability
CVE-2019-1362 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1363 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1364 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1365 - Microsoft IIS Server Elevation of Privilege Vulnerability
CVE-2019-1368 - Windows Secure Boot Security Feature Bypass Vulnerability
CVE-2019-1369 - Open Enclave SDK Information Disclosure Vulnerability
CVE-2019-1372 - Azure App Service Remote Code Execution Vulnerability
CVE-2019-1376 - SQL Server Management Studio Information Disclosure Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems

Windows Server, version 1903 (Server Core installation)
Azure App Service on Azure Stack
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Open Enclave SDK
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
SQL Server Management Studio 18.3
Windows 8.1 for 32-bit systems
Windows 10 Mobile
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1903 for 32-bit Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Server, version 1803 (Server Core Installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
SQL Server Management Studio 18.3.1

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1339
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1321
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1364
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1343
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1323
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1326
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1359
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1372
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1316
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1318
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1358
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1345
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1320
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1369
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1341
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1344
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1314
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1362
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1319
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1322
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1317
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1365
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1346
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1060

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1376
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1375
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1347
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1166
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1342
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1311
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1333
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1338
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1337
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1363
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1361
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1230
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1340
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1336
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1315
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1368
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1334
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1325
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1313
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1060
URL	https://support.microsoft.com/en-us/help/4519976
URL	https://support.microsoft.com/en-us/help/4519338
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001

Type	Reference
URL	https://support.microsoft.com/en-us/help/4516655
URL	https://support.microsoft.com/en-us/help/4520010
URL	https://support.microsoft.com/en-us/help/4520004
URL	https://support.microsoft.com/en-us/help/4520007
URL	https://support.microsoft.com/en-us/help/4517389
URL	https://support.microsoft.com/en-us/help/4520008
URL	https://support.microsoft.com/en-us/help/4520005
URL	https://support.microsoft.com/en-us/help/4519998
URL	https://support.microsoft.com/en-us/help/4520002
URL	https://support.microsoft.com/en-us/help/4520011
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1313
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1325
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1334
URL	https://support.microsoft.com/en-us/help/4512939
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1368
URL	https://support.microsoft.com/en-us/help/4517134
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1315
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1340
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1336
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1230

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1343
URL	https://support.microsoft.com/en-us/help/4512938
URL	https://support.microsoft.com/en-us/help/4521858
URL	https://support.microsoft.com/en-us/help/4521863
URL	https://support.microsoft.com/en-us/help/4521862
URL	https://support.microsoft.com/en-us/help/4521860
URL	https://support.microsoft.com/en-us/help/4520009
URL	https://support.microsoft.com/en-us/help/4521856
URL	https://support.microsoft.com/en-us/help/4520003
URL	https://support.microsoft.com/en-us/help/4519985
URL	https://support.microsoft.com/en-us/help/4515519
URL	https://support.microsoft.com/en-us/help/4521859
URL	https://support.microsoft.com/en-us/help/4521861
URL	https://support.microsoft.com/en-us/help/4519990
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1323
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1326
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1359
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1361
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1339
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1364

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1338
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1363
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1337
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1372
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1316
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1318
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1333
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1321
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1358
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1345
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1311
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1342
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1166
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1347
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1320
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1369

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1341
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1344
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1314
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1362
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1375
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1319
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1322
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1317
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1365
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1346
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1376

MS19-SEP: Microsoft Internet Explorer Out-of-Band Security Update — High

Vulnerability Details

Microsoft has released an out-of-band security update for Internet Explorer which includes a fix for the following vulnerability:

CVE-2019-1367 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 9 on Windows Server 2008 for x64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems
Internet Explorer 10 on Windows Server 2012 for x64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems

Internet Explorer 11 on Windows Server 2008 R2 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows RT 8.1 for x64-based systems
Internet Explorer 11 on Windows RT 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2 for x64-based Systems
Internet Explorer 11 on Windows Server 2012 R2 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1507 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1507 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems

Solution Details

Microsoft has released a fix for this flaw in their September 2019 out-of-band Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1367
URL	https://support.microsoft.com/help/4522011
URL	https://support.microsoft.com/help/4522010
URL	https://support.microsoft.com/help/4522009
URL	https://support.microsoft.com/help/4522007

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1367
URL	https://support.microsoft.com/help/4522012
URL	https://support.microsoft.com/help/4522016
URL	https://support.microsoft.com/help/4522015
URL	https://support.microsoft.com/help/4522014

MS19-SEP: Microsoft Internet Explorer Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-1208 - VBScript Remote Code Execution Vulnerability
CVE-2019-1220 - Microsoft Browser Security Feature Bypass Vulnerability
CVE-2019-1221 - Scripting Engine Memory Corruption Vulnerability
CVE-2019-1236 - VBScript Remote Code Execution Vulnerability

Affected Products:
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems

Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their September 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1221
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1208
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1220

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1236
URL	https://support.microsoft.com/en-us/help/4516044
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1221
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1208
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1220
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1236
URL	https://support.microsoft.com/en-us/help/4516070
URL	https://support.microsoft.com/en-us/help/4512578
URL	https://support.microsoft.com/en-us/help/4516066
URL	https://support.microsoft.com/en-us/help/4516065
URL	https://support.microsoft.com/en-us/help/4516067
URL	https://support.microsoft.com/en-us/help/4516068
URL	https://support.microsoft.com/en-us/help/4516026
URL	https://support.microsoft.com/en-us/help/4516055
URL	https://support.microsoft.com/en-us/help/4516046
URL	https://support.microsoft.com/en-us/help/4515384
URL	https://support.microsoft.com/en-us/help/4516058

MS19-SEP: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2019-0928 - Windows Hyper-V Denial of Service Vulnerability
CVE-2019-1209 - Lync 2013 Information Disclosure Vulnerability

CVE-2019-1214 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2019-1215 - Windows Elevation of Privilege Vulnerability
CVE-2019-1216 - DirectX Information Disclosure Vulnerability
CVE-2019-1219 - Windows Transaction Manager Information Disclosure Vulnerability
CVE-2019-1231 - Rome SDK Information Disclosure Vulnerability
CVE-2019-1232 - Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2019-1267 - Microsoft Compatibility Appraiser Elevation of Privilege Vulnerability
CVE-2019-1268 - Winlogon Elevation of Privilege Vulnerability
CVE-2019-1269 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2019-1270 - Microsoft Windows Store Installer Elevation of Privilege Vulnerability
CVE-2019-1271 - Windows Media Elevation of Privilege Vulnerability
CVE-2019-1272 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2019-1273 - Active Directory Federation Services XSS Vulnerability
CVE-2019-1274 - Windows Kernel Information Disclosure Vulnerability
ADV990001 - Latest Servicing Stack Updates
CVE-2019-0787 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2019-0788 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2019-1235 - Windows Text Service Framework Elevation of Privilege Vulnerability
CVE-2019-1240 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1241 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1242 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1243 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1244 - DirectWrite Information Disclosure Vulnerability
CVE-2019-1245 - DirectWrite Information Disclosure Vulnerability
CVE-2019-1247 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1248 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1249 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1250 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2019-1251 - DirectWrite Information Disclosure Vulnerability
CVE-2019-1252 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1253 - Windows Elevation of Privilege Vulnerability
CVE-2019-1254 - Windows Hyper-V Information Disclosure Vulnerability
CVE-2019-1256 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1265 - Microsoft Yammer Security Feature Bypass Vulnerability
CVE-2019-1277 - Windows Audio Service Elevation of Privilege Vulnerability
CVE-2019-1278 - Windows Elevation of Privilege Vulnerability
CVE-2019-1280 - LNK Remote Code Execution Vulnerability
CVE-2019-1282 - Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2019-1283 - Microsoft Graphics Components Information Disclosure Vulnerability
CVE-2019-1284 - DirectX Elevation of Privilege Vulnerability
CVE-2019-1285 - Win32k Elevation of Privilege Vulnerability
CVE-2019-1286 - Windows GDI Information Disclosure Vulnerability
CVE-2019-1287 - Windows Network Connectivity Assistant Elevation of Privilege Vulnerability
CVE-2019-1289 - Windows Update Delivery Optimization Elevation of Privilege Vulnerability
CVE-2019-1290 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2019-1291 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2019-1292 - Windows Denial of Service Vulnerability
CVE-2019-1293 - Windows SMB Client Driver Information Disclosure Vulnerability
CVE-2019-1294 - Windows Secure Boot Security Feature Bypass Vulnerability

CVE-2019-1301 - .NET Core Denial of Service Vulnerability
CVE-2019-1302 - ASP.NET Core Elevation Of Privilege Vulnerability
CVE-2019-1303 - Windows Elevation of Privilege Vulnerability
CVE-2019-1305 - Team Foundation Server Cross-site Scripting Vulnerability
CVE-2019-1306 - Azure DevOps and Team Foundation Server Remote Code Execution Vulnerability

Affected Products:
ASP.NET Core 2.1
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
ASP.NET Core 3.0
Windows 10 Version 1607 for 32-bit Systems
Rome SDK 1.4.1
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
ASP.NET Core 2.2
Microsoft Visual Studio 2019 version 16.0
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1703 for x64-based Systems
Microsoft Lync Server 2013
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Microsoft Visual Studio 2017 version 15.9
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Azure DevOps Server 2019 Update 1
Team Foundation Server 2017 Update 3.1
Windows 10 Version 1903 for 32-bit Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft Visual Studio 2019 version 16.2
Team Foundation Server 2018 Update 3.2
.NET Core 2.1
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Yammer for Android

Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Azure DevOps Server 2019.0.1
Microsoft Visual Studio 2015 Update 3
Windows 10 Version 1703 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Team Foundation Server 2018 Update 1.2
.NET Core 2.2
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Team Foundation Server 2015 Update 4.2
Microsoft Visual Studio 2017 version 15.0
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Solution Details

Microsoft has released a fix for this flaw in their September 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1270
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1271
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1243
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1241
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1242
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1252
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1256
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1272
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1292

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1254
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0787
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1302
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1286
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1219
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1250
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1267
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0788
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1245
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1273
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1231
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1293
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1306
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1248
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1268
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1240
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1247
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1303
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1215
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1214
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1294
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1285
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1274
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1269

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1235
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0928
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1209
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1249
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1284
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1277
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1251
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1287
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1291
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1232
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1244
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1216
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1278
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1280
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1301
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1253
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1282
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1290
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1265
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1289
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1305
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-1283
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1290

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1282
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1265
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1289
URL	https://support.microsoft.com/en-us/help/4516033
URL	https://support.microsoft.com/en-us/help/4515383
URL	https://support.microsoft.com/en-us/help/4516051
URL	https://support.microsoft.com/en-us/help/4512577
URL	https://support.microsoft.com/en-us/help/4513696
URL	https://support.microsoft.com/en-us/help/4517134
URL	https://support.microsoft.com/en-us/help/4512939
URL	https://support.microsoft.com/en-us/help/4512573
URL	https://support.microsoft.com/en-us/help/4512575
URL	https://support.microsoft.com/en-us/help/4516655
URL	https://support.microsoft.com/en-us/help/4516062
URL	https://support.microsoft.com/en-us/help/4512574
URL	https://support.microsoft.com/en-us/help/4512938
URL	https://support.microsoft.com/en-us/help/4515509
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0928
URL	https://support.microsoft.com/en-us/help/4516064
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1277
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1284

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1249
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1209
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1214
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1294
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1285
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1274
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1269
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1283
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1235
URL	https://support.microsoft.com/en-us/help/4512576
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1305
URL	https://support.microsoft.com/en-us/help/4511839
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1271
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1243
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1242
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1272

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV990001
URL	https://support.microsoft.com/en-us/help/4516070
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1292
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0787
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1302
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1286
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1219
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1250
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1267
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0788
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1245
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1241
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1252
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1256
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1273
URL	https://support.microsoft.com/en-us/help/4516044
URL	https://support.microsoft.com/en-us/help/4516058

Type	Reference
URL	https://support.microsoft.com/en-us/help/4512578
URL	https://support.microsoft.com/en-us/help/4516066
URL	https://support.microsoft.com/en-us/help/4516065
URL	https://support.microsoft.com/en-us/help/4516067
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1254
URL	https://support.microsoft.com/en-us/help/4516068
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1215
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1303
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1247
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1240
URL	https://support.microsoft.com/en-us/help/4516026
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1268
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1248
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1306
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1253
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1301
URL	https://support.microsoft.com/en-us/help/4516055
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1280

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1278
URL	https://support.microsoft.com/en-us/help/4515384
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1216
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1244
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1232
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1293
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1291
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1287
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1270
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1231
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1251

MS20-APR: Microsoft Internet Explorer Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their April 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-0895 - Windows VBScript Engine Remote Code Execution Vulnerability
CVE-2020-0966 - VBScript Remote Code Execution Vulnerability
CVE-2020-0967 - VBScript Remote Code Execution Vulnerability
CVE-2020-0968 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2012
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0966
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0895
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0967

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0968
URL	https://support.microsoft.com/en-us/help/4549951
URL	https://support.microsoft.com/en-us/help/4549949
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0895
URL	https://support.microsoft.com/en-us/help/4550964
URL	https://support.microsoft.com/en-us/help/4550922
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0966
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0967
URL	https://support.microsoft.com/en-us/help/4550905
URL	https://support.microsoft.com/en-us/help/4550930
URL	https://support.microsoft.com/en-us/help/4550961
URL	https://support.microsoft.com/en-us/help/4550927
URL	https://support.microsoft.com/en-us/help/4550929
URL	https://support.microsoft.com/en-us/help/4550917
URL	https://support.microsoft.com/en-us/help/4550951
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0968

MS20-APR: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their April 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-0784 - DirectX Elevation of Privilege Vulnerability
CVE-2020-0794 - Windows Denial of Service Vulnerability
CVE-2020-0835 - Windows Defender Antimalware Platform Hard Link Elevation of Privilege Vulnerability
CVE-2020-0899 - Microsoft Visual Studio Elevation of Privilege Vulnerability
CVE-2020-0907 - Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-0910 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2020-0913 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0917 - Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2020-0918 - Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2020-0935 - OneDrive for Windows Elevation of Privilege Vulnerability
CVE-2020-0944 - Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-0945 - Media Foundation Information Disclosure Vulnerability
CVE-2020-0946 - Media Foundation Information Disclosure Vulnerability
CVE-2020-0947 - Media Foundation Information Disclosure Vulnerability
CVE-2020-0948 - Media Foundation Memory Corruption Vulnerability
CVE-2020-0949 - Media Foundation Memory Corruption Vulnerability
CVE-2020-0950 - Media Foundation Memory Corruption Vulnerability
CVE-2020-0955 - Windows Kernel Information Disclosure in CPU Memory Access
CVE-2020-0985 - Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-0987 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-0988 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0992 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0993 - Windows DNS Denial of Service Vulnerability
CVE-2020-0994 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0995 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0996 - Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-0999 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1000 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1001 - Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-1002 - Microsoft Defender Elevation of Privilege Vulnerability
CVE-2020-1003 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1004 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-1005 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-1006 - Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-1007 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1008 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1018 - Microsoft Dynamics Business Central/NAV Information Disclosure
CVE-2020-1019 - Microsoft RMS Sharing App for Mac Elevation of Privilege Vulnerability
CVE-2020-1026 - MSR JavaScript Cryptography Library Security Feature Bypass Vulnerability
CVE-2020-1027 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1029 - Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-0687 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2020-0699 - Win32k Information Disclosure Vulnerability
CVE-2020-0821 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-0888 - DirectX Elevation of Privilege Vulnerability
CVE-2020-0889 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0900 - Visual Studio Extension Installer Service Elevation of Privilege Vulnerability
CVE-2020-0919 - Microsoft Remote Desktop App for Mac Elevation of Privilege Vulnerability
CVE-2020-0934 - Windows Elevation of Privilege Vulnerability

CVE-2020-0936 - Windows Scheduled Task Elevation of Privilege Vulnerability
CVE-2020-0937 - Media Foundation Information Disclosure Vulnerability
CVE-2020-0938 - Adobe Font Manager Library Remote Code Execution Vulnerability
CVE-2020-0939 - Media Foundation Information Disclosure Vulnerability
CVE-2020-0940 - Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-0942 - Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-0943 - Microsoft YourPhone Application for Android Authentication Bypass Vulnerability
CVE-2020-0952 - Windows GDI Information Disclosure Vulnerability
CVE-2020-0953 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0956 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0957 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0958 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0959 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0960 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-0962 - Win32k Information Disclosure Vulnerability
CVE-2020-0964 - GDI+ Remote Code Execution Vulnerability
CVE-2020-0965 - Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2020-0981 - Windows Token Security Feature Bypass Vulnerability
CVE-2020-0982 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-0983 - Windows Elevation of Privilege Vulnerability
CVE-2020-0984 - Microsoft (MAU) Office Elevation of Privilege Vulnerability
CVE-2020-1009 - Windows Elevation of Privilege Vulnerability
CVE-2020-1011 - Windows Elevation of Privilege Vulnerability
CVE-2020-1014 - Microsoft Windows Update Client Elevation of Privilege Vulnerability
CVE-2020-1015 - Windows Elevation of Privilege Vulnerability
CVE-2020-1016 - Windows Push Notification Service Information Disclosure Vulnerability
CVE-2020-1017 - Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-1020 - Adobe Font Manager Library Remote Code Execution Vulnerability
CVE-2020-1022 - Dynamics Business Central Remote Code Execution Vulnerability
CVE-2020-1049 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-1094 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-1050 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows Defender on Windows Server 2019
Windows Defender on Windows Server 2012
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Microsoft Remote Desktop for Mac
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Defender on Windows 10 Version 1803 for ARM64-based Systems
Dynamics 365 Business Central 2019 Spring Update
Windows Server 2019

Windows Defender on Windows Server 2016 (Server Core installation)
Windows Defender on Windows Server, version 1803 (Server Core Installation)
Microsoft Visual Studio 2019 version 16.0
Microsoft System Center 2012 R2 Endpoint Protection
Windows Defender on Windows Server 2012 R2 (Server Core installation)
Windows Defender on Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows Defender on Windows 10 Version 1903 for x64-based Systems
Dynamics 365 Server, version 9.0 (on-premises)
Windows Defender on Windows Server 2016
Windows 8.1 for x64-based systems
Windows Defender on Windows 7 for 32-bit Systems Service Pack 1
OneDrive for Windows
Windows Defender on Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2015 Update 3
Microsoft RMS Sharing for Mac
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Security Essentials
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows Defender on Windows 10 for 32-bit Systems
Windows Defender on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Defender on Windows 10 Version 1803 for x64-based Systems
Windows Defender on Windows 10 for x64-based Systems
Microsoft AutoUpdate for Mac
Windows 10 Version 1809 for x64-based Systems
Microsoft Visual Studio 2019 version 16.5
Microsoft Dynamics 365 BC On Premise
Microsoft System Center 2012 Endpoint Protection
Microsoft Forefront Endpoint Protection 2010
Windows Defender on Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1709 for ARM64-based Systems
Windows Defender on Windows 10 Version 1903 for ARM64-based Systems
Dynamics 365 Business Central 2019 Release Wave 2 (On-Premise)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1

Windows Defender on Windows 10 Version 1803 for 32-bit Systems
Windows Defender on Windows 10 Version 1903 for 32-bit Systems
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft Dynamics NAV 2015
Windows Defender on Windows 10 Version 1607 for 32-bit Systems
Windows Defender on Windows 10 Version 1909 for ARM64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Defender antimalware platform
Windows 10 Version 1709 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for x64-based Systems
Microsoft Dynamics NAV 2013
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1607 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows 8.1 for x64-based systems
Windows Defender on Windows Server 2019 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Defender on Windows Server, version 1909 (Server Core installation)
Microsoft Your Phone Companion App for Android
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1909 for ARM64-based Systems
Windows Defender on Windows Server, version 1903 (Server Core installation)
Microsoft Dynamics NAV 2016
Microsoft Dynamics NAV 2018
Windows 10 Version 1709 for ARM64-based Systems
Microsoft Research JavaScript Cryptography Library V1.4
Microsoft Dynamics NAV 2017
Windows Defender on Windows 10 Version 1809 for 32-bit Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Windows Defender on Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows Defender on Windows Server 2012 R2
Windows 10 Version 1803 for ARM64-based Systems
Windows Defender on Windows 10 Version 1809 for ARM64-based Systems
Microsoft System Center Endpoint Protection
Windows Defender on Windows Server 2012 (Server Core installation)
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows 7 for x64-based Systems Service Pack 1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0955
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1026
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0947
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0992
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0995
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1007
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0965
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0907
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0940
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1014
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0953
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0952
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0943
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0917
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0946
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1027
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0945
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0987
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1029
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0985
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1016

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0994
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0899
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0982
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0821
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1004
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1050
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0888
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0918
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0949
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1015
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0981
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1005
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0934
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1019
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0950
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0948
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1003
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0687
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0988
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0936
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1008
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0699
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0794
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0984

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0962
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0996
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0910
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1001
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0999
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1020
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0937
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1011
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0784
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0913
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1022
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1049
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0935
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1000
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0993
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0956
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1002
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0889
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0959
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0944
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0957
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0983
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0942
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1018

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0938
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0835
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1017
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0939
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1006
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1009
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0900
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1094
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0919
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0958
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0964
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0960
URL	https://support.microsoft.com/en-us/help/4550957
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0888
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0937
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0958
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0995
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1001
URL	https://support.microsoft.com/en-us/help/4550951
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1008
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1016

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1029
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0987
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1049
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0950
URL	https://support.microsoft.com/en-us/help/4549674
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0934
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1005
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1015
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0985
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0992
URL	https://support.microsoft.com/en-us/help/4549949
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1000
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1014
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0947
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1007
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0962
URL	https://support.microsoft.com/en-us/help/4550965

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0993
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0965
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0959
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0907
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0940
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0983
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0942
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1018
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0953
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0938
URL	https://support.microsoft.com/en-us/help/4557699
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0982
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0952
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1020
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1011
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0913

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0910
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0936
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0957
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0943
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0946
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0917
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1022
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0794
URL	https://support.microsoft.com/en-us/help/4550964
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0984
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1026
URL	https://support.microsoft.com/en-us/help/4549678
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0960
URL	https://support.microsoft.com/en-us/help/4550970
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1094
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1027
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0835

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1017
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0784
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0939
URL	https://support.microsoft.com/en-us/help/4540102
URL	https://support.microsoft.com/en-us/help/4557700
URL	https://support.microsoft.com/en-us/help/4549675
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0949
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0699
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1050
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0919
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0945
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0899
URL	https://support.microsoft.com/en-us/help/4549676
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1004
URL	https://support.microsoft.com/en-us/help/4549673
URL	https://support.microsoft.com/en-us/help/4550917
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0889
URL	https://support.microsoft.com/en-us/help/4550929

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0956
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1002
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0918
URL	https://support.microsoft.com/en-us/help/4550927
URL	https://support.microsoft.com/en-us/help/4550971
URL	https://support.microsoft.com/en-us/help/4549951
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0948
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0821
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0935
URL	https://support.microsoft.com/en-us/help/4550922
URL	https://support.microsoft.com/en-us/help/4538593
URL	https://support.microsoft.com/en-us/help/4550930
URL	https://support.microsoft.com/en-us/help/4550961
URL	https://support.microsoft.com/en-us/help/4549677
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0955
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0999
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0964
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1019
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0687

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1006
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0981
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0900
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1009
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0988
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0996
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0994
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0944
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1003

MS20-AUG: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their August 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-1380 - Scripting Engine Memory Corruption Vulnerability
CVE-2020-1567 - MSHTML Engine Remote Code Execution Vulnerability
CVE-2020-1570 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems

Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for ARM64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 2004 for 32-bit Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1567
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1380
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1570
URL	https://support.microsoft.com/en-us/help/4571729

Type	Reference
URL	https://support.microsoft.com/en-us/help/4565349
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1380
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1567
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1570
URL	https://support.microsoft.com/en-us/help/4571694
URL	https://support.microsoft.com/en-us/help/4566782
URL	https://support.microsoft.com/en-us/help/4571730
URL	https://support.microsoft.com/en-us/help/4571703
URL	https://support.microsoft.com/en-us/help/4571709
URL	https://support.microsoft.com/en-us/help/4565351
URL	https://support.microsoft.com/en-us/help/4571687
URL	https://support.microsoft.com/en-us/help/4571741
URL	https://support.microsoft.com/en-us/help/4571736
URL	https://support.microsoft.com/en-us/help/4571692

MS20-AUG: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their August 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-1417 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1464 - Windows Spoofing Vulnerability
CVE-2020-1470 - Windows Work Folders Service Elevation of Privilege Vulnerability
CVE-2020-1509 - Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
CVE-2020-1510 - Win32k Information Disclosure Vulnerability

CVE-2020-1516 - Windows Work Folders Service Elevation of Privilege Vulnerability
CVE-2020-1517 - Windows File Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2020-1518 - Windows File Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2020-1519 - Windows UPnP Device Host Elevation of Privilege Vulnerability
CVE-2020-1520 - Windows Font Driver Host Remote Code Execution Vulnerability
CVE-2020-1521 - Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2020-1522 - Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2020-1524 - Windows Speech Shell Components Elevation of Privilege Vulnerability
CVE-2020-1525 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1526 - Windows Network Connection Broker Elevation of Privilege Vulnerability
CVE-2020-1527 - Windows Custom Protocol Engine Elevation of Privilege Vulnerability
CVE-2020-1528 - Windows Radio Manager API Elevation of Privilege Vulnerability
CVE-2020-1529 - Windows GDI Elevation of Privilege Vulnerability
CVE-2020-1530 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-1531 - Windows Accounts Control Elevation of Privilege Vulnerability
CVE-2020-1533 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1534 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-1535 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1536 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1537 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-1538 - Windows UPnP Device Host Elevation of Privilege Vulnerability
CVE-2020-1539 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1540 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1541 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1542 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1543 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1544 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1545 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1546 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1547 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1548 - Windows WaasMedic Service Information Disclosure Vulnerability
CVE-2020-1549 - Windows CDP User Components Elevation of Privilege Vulnerability
CVE-2020-1550 - Windows CDP User Components Elevation of Privilege Vulnerability
CVE-2020-1377 - Windows Registry Elevation of Privilege Vulnerability
CVE-2020-1378 - Windows Registry Elevation of Privilege Vulnerability
CVE-2020-1379 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1383 - Windows RRAS Service Information Disclosure Vulnerability
CVE-2020-1455 - Microsoft SQL Server Management Studio Denial of Service Vulnerability
CVE-2020-1459 - Windows ARM Information Disclosure Vulnerability
CVE-2020-1339 - Windows Media Remote Code Execution Vulnerability
CVE-2020-1337 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-1466 - Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability
CVE-2020-1467 - Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-1472 - Netlogon Elevation of Privilege Vulnerability
CVE-2020-1473 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1474 - Windows Image Acquisition Service Information Disclosure Vulnerability
CVE-2020-1475 - Windows Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2020-1477 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1478 - Media Foundation Memory Corruption Vulnerability

CVE-2020-1479 - DirectX Elevation of Privilege Vulnerability
CVE-2020-1480 - Windows GDI Elevation of Privilege Vulnerability
CVE-2020-1484 - Windows Work Folders Service Elevation of Privilege Vulnerability
CVE-2020-1485 - Windows Image Acquisition Service Information Disclosure Vulnerability
CVE-2020-1486 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1487 - Media Foundation Information Disclosure Vulnerability
CVE-2020-1488 - Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
CVE-2020-1489 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2020-1490 - Windows Storage Service Elevation of Privilege Vulnerability
CVE-2020-1492 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1511 - Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-1512 - Windows State Repository Service Information Disclosure Vulnerability
CVE-2020-1513 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2020-1515 - Windows Telephony Server Elevation of Privilege Vulnerability
CVE-2020-1551 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-1552 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-1553 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1554 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1556 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1557 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1558 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1560 - Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2020-1561 - Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1562 - Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1564 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1565 - Windows Elevation of Privilege Vulnerability
CVE-2020-1566 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1571 - Windows Setup Elevation of Privilege Vulnerability
CVE-2020-1574 - Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2020-1577 - DirectWrite Information Disclosure Vulnerability
CVE-2020-1578 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1579 - Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability
CVE-2020-1584 - Windows dnsrslvr.dll Elevation of Privilege Vulnerability
CVE-2020-1585 - Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2020-1587 - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2020-1591 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-1597 - ASP.NET Core Denial of Service Vulnerability
CVE-2020-0604 - Visual Studio Code Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)

Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
Windows 10 Version 1803 for x64-based Systems
Windows 8.1 for x64-based systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 1903 for ARM64-based Systems
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows 10 Version 1809 for x64-based Systems
ASP.NET Core 2.1
SQL Server Management Studio 18.6
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
ASP.NET Core 3.1
Windows Server, version 1909 (Server Core installation)
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1486
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1455
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1511
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1464
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1477
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1378
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1541
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1527
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1562
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1548
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1470
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1556
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1552
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1521
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1517
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1459
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1339
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1490
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0604
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1526
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1549
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1574
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1536

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1542
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1566
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1509
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1522
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1337
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1417
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1479
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1524
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1529
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1513
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1553
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1466
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1561
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1520
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1487
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1538
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1489
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1379
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1478
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1473
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1488
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1510
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1534
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1525

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1565
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1535
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1585
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1383
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1579
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1584
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1558
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1485
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1377
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1516
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1597
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1544
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1474
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1484
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1480
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1550
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1492
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1578
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1554
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1537
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1557
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1518
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1551
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1564

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1519
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1560
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1539
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1530
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1528
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1545
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1543
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1577
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1472
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1533
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1571
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1547
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1546
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1512
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1515
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1540
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1531
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1467
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1591
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1587
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1475
URL	https://support.microsoft.com/en-us/help/4571694
URL	https://support.microsoft.com/en-us/help/4566782
URL	https://support.microsoft.com/en-us/help/4565349

Type	Reference
URL	https://support.microsoft.com/en-us/help/4571729
URL	https://support.microsoft.com/en-us/help/4571692
URL	https://support.microsoft.com/en-us/help/4571736
URL	https://support.microsoft.com/en-us/help/4571741
URL	https://support.microsoft.com/en-us/help/4565351
URL	https://support.microsoft.com/en-us/help/4571709
URL	https://support.microsoft.com/en-us/help/4571703
URL	https://support.microsoft.com/en-us/help/4571730
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1511
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1455
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1464
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1477
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1378
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1541
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1527
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1562
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1548
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1556
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1470

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1552
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1521
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1517
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1339
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1459
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0604
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1490
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1526
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1549
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1574
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1536
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1542
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1566
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1509
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1522
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1337

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1417
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1479
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1524
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1553
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1513
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1529
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1466
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1561
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1487
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1520
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1538
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1489
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1478
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1379
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1488
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1473

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1510
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1534
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1525
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1486
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1565
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1535
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1585
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1383
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1579
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1584
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1558
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1485
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1377
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1516
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1597
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1544

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1474
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1484
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1480
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1550
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1492
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1578
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1554
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1537
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1557
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1518
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1564
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1551
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1560
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1519
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1528
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1530

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1539
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1577
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1543
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1545
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1571
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1533
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1546
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1547
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1515
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1512
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1531
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1540
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1591
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1467
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1587

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1475
URL	https://support.microsoft.com/en-us/help/4571719
URL	https://support.microsoft.com/en-us/help/4541722
URL	https://support.microsoft.com/en-us/help/4571702
URL	https://support.microsoft.com/en-us/help/4571746
URL	https://support.microsoft.com/en-us/help/4571723

MS20-DEC: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their December 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-17092 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-17094 - Windows Error Reporting Information Disclosure Vulnerability
CVE-2020-17095 - Hyper-V Remote Code Execution Vulnerability
CVE-2020-17096 - Windows NTFS Remote Code Execution Vulnerability
CVE-2020-17097 - Windows Digital Media Receiver Elevation of Privilege Vulnerability
CVE-2020-17098 - Windows GDI+ Information Disclosure Vulnerability
CVE-2020-17099 - Windows Lock Screen Security Feature Bypass Vulnerability
CVE-2020-17103 - Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2020-17134 - Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2020-17135 - Azure DevOps Server Spoofing Vulnerability
CVE-2020-17136 - Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2020-17137 - DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2020-17138 - Windows Error Reporting Information Disclosure Vulnerability
CVE-2020-17139 - Windows Overlay Filter Security Feature Bypass Vulnerability
CVE-2020-17147 - Dynamics CRM Webclient Cross-site Scripting Vulnerability
CVE-2020-17148 - Visual Studio Code Remote Development Extension Remote Code Execution Vulnerability
CVE-2020-17150 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2020-17152 - Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability
CVE-2020-17156 - Visual Studio Remote Code Execution Vulnerability
CVE-2020-17158 - Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code

Execution Vulnerability
CVE-2020-17159 - Visual Studio Code Java Extension Pack Remote Code Execution Vulnerability
CVE-2020-17160 - Azure Sphere Security Feature Bypass Vulnerability
ADV200013 - Microsoft Guidance for Addressing Spoofing Vulnerability in DNS Resolver
CVE-2020-16958 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16959 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16960 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16961 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16962 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16963 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16964 - Windows Backup Engine Elevation of Privilege Vulnerability
CVE-2020-16971 - Azure SDK for Java Security Feature Bypass Vulnerability
CVE-2020-16996 - Kerberos Security Feature Bypass Vulnerability
CVE-2020-17002 - Azure SDK for C Security Feature Bypass Vulnerability
CVE-2020-17133 - Microsoft Dynamics Business Central/NAV Information Disclosure
CVE-2020-17140 - Windows SMB Information Disclosure Vulnerability
CVE-2020-17145 - Azure DevOps Server and Team Foundation Services Spoofing Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows 10 Version 20H2 for 32-bit Systems
Visual Studio Code Language Support for Java Extension
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
Windows 10 Version 1803 for x64-based Systems
Windows 8.1 for x64-based systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Team Foundation Server 2018 Update 3.2
Windows 10 Version 1803 for 32-bit Systems
Microsoft Dynamics 365 (on-premises) version 8.2
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Azure DevOps Server 2019.0.1
Windows 10 Version 2004 for ARM64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2

Windows 10 for x64-based Systems
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 1903 for ARM64-based Systems
C SDK for Azure IoT
Azure Sphere
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows 10 Version 1809 for x64-based Systems
Azure DevOps Server 2020
Windows Server, version 20H2 (Server Core Installation)
Dynamics 365 for Finance and Operations
Visual Studio Code TS-Lint Extension
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Microsoft Dynamics NAV 2015
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Server, version 1909 (Server Core installation)
Team Foundation Server 2017 Update 3.1
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Visual Studio Code Remote - SSH Extension
Team Foundation Server 2018 Update 1.2
Windows 10 Version 1803 for ARM64-based Systems
Microsoft Visual Studio 2019 version 16.8
Windows Server 2019 (Server Core installation)
Azure SDK for Java
Windows Server 2016
Team Foundation Server 2015 Update 4.2
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Azure DevOps Server 2019 Update 1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.9

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17103

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16971
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16963
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17140
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17159
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17148
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17158
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16960
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16996
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17134
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17137
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16959
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17156
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17139
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17138
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17095
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17150
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17098
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17136
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17152
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17097
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16962
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17099
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16958

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17135
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17092
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16964
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16961
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17094
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17002
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17133
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17096
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17147
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17139
URL	https://support.microsoft.com/en-us/help/4592468
URL	https://support.microsoft.com/en-us/help/4595462
URL	https://support.microsoft.com/en-us/help/4592498
URL	https://support.microsoft.com/en-us/help/4592446
URL	https://support.microsoft.com/en-us/help/4592471
URL	https://support.microsoft.com/en-us/help/4592503
URL	https://support.microsoft.com/en-us/help/4592464
URL	https://support.microsoft.com/en-us/help/4593226
URL	https://support.microsoft.com/en-us/help/4592504
URL	https://support.microsoft.com/en-us/help/4595459
URL	https://support.microsoft.com/en-us/help/4592440
URL	https://support.microsoft.com/en-us/help/4592495
URL	https://support.microsoft.com/en-us/help/4586793
URL	https://support.microsoft.com/en-us/help/4586830

Type	Reference
URL	https://support.microsoft.com/en-us/help/4586781
URL	https://support.microsoft.com/en-us/help/4586786
URL	https://support.microsoft.com/en-us/help/4592449
URL	https://support.microsoft.com/en-us/help/4592484
URL	https://support.microsoft.com/en-us/help/4592438
URL	https://support.microsoft.com/en-us/help/4592497
URL	https://support.microsoft.com/en-us/help/4583556
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16963
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17140
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17159
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200013
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17148
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17158
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16960
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16996
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17134
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17137
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16959

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17156
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17138
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17095
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17145
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17150
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17098
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17136
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17152
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17097
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16962
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17099
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16958
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17135
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17092
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16964
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16961

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17160
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17094
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17002
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17133
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17096
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17147
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17103
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16971

MS20-FEB: Microsoft Internet Explorer Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their February 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-0673 - Scripting Engine Memory Corruption Vulnerability
CVE-2020-0674 - Scripting Engine Memory Corruption Vulnerability
CVE-2020-0706 - Microsoft Browser Information Disclosure Vulnerability

Affected Products:
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for x64-based Systems

Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0673
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0674
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0706
URL	https://support.microsoft.com/en-us/help/4537814
URL	https://support.microsoft.com/en-us/help/4532693
URL	https://support.microsoft.com/en-us/help/4537764
URL	https://support.microsoft.com/en-us/help/4537820
URL	https://support.microsoft.com/en-us/help/4537789
URL	https://support.microsoft.com/en-us/help/4537762
URL	https://support.microsoft.com/en-us/help/4537776
URL	https://support.microsoft.com/en-us/help/4537767
URL	https://support.microsoft.com/en-us/help/4537821
URL	https://support.microsoft.com/en-us/help/4532691
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0706
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0673
URL	https://support.microsoft.com/en-us/help/4537810
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0674

MS20-FEB: Microsoft SQL Server Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their February 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft SQL Server which include fixes for the following vulnerabilities:

CVE-2020-0618 - Microsoft SQL Server Reporting Services Remote Code Execution Vulnerability

Affected Products:
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (GDR)
Microsoft SQL Server 2012 for x64-based Systems Service Pack 4 (QFE)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (CU)
Microsoft SQL Server 2012 for 32-bit Systems Service Pack 4 (QFE)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)

CVSS Base Score: 6.5

CVSS Vector: AV:N/AC:L/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0618
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0618
URL	https://support.microsoft.com/en-us/help/4532095
URL	https://support.microsoft.com/en-us/help/4535706
URL	https://support.microsoft.com/en-us/help/4532097
URL	https://support.microsoft.com/en-us/help/4535288
URL	https://support.microsoft.com/en-us/help/4532098

MS20-FEB: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their February 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-0655 - Remote Desktop ServicesÂ Remote Code Execution Vulnerability

CVE-2020-0660 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2020-0661 - Windows Hyper-V Denial of Service Vulnerability
CVE-2020-0662 - Windows Remote Code Execution Vulnerability
CVE-2020-0665 - Active Directory Elevation of Privilege Vulnerability
CVE-2020-0666 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0667 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0668 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0669 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0670 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0671 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0672 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0675 - Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0676 - Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0677 - Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0678 - Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2020-0679 - Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-0680 - Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-0681 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2020-0682 - Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-0683 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0685 - Windows COM Server Elevation of Privilege Vulnerability
CVE-2020-0686 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0691 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0701 - Windows Client License Service Elevation of Privilege Vulnerability
CVE-2020-0702 - Surface Hub Security Feature Bypass Vulnerability
CVE-2020-0727 - Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-0728 - Windows Modules Installer Service Information Disclosure Vulnerability
CVE-2020-0729 - LNK Remote Code Execution Vulnerability
CVE-2020-0730 - Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2020-0733 - Windows Malicious Software Removal Tool Elevation of Privilege Vulnerability
CVE-2020-0734 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2020-0735 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0736 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-0737 - Windows Elevation of Privilege Vulnerability
CVE-2020-0738 - Media Foundation Memory Corruption Vulnerability
CVE-2020-0739 - Windows Elevation of Privilege Vulnerability
CVE-2020-0740 - Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0741 - Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0742 - Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0743 - Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0745 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0746 - Microsoft Graphics Components Information Disclosure Vulnerability
CVE-2020-0747 - Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2020-0748 - Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0749 - Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0750 - Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-0751 - Windows Hyper-V Denial of Service Vulnerability
CVE-2020-0752 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0753 - Windows Error Reporting Elevation of Privilege Vulnerability

CVE-2020-0754 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-0755 - Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0756 - Windows Key Isolation Service Information Disclosure Vulnerability
CVE-2020-0757 - Windows SSH Elevation of Privilege Vulnerability
CVE-2020-0792 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0657 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-0658 - Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2020-0659 - Windows Data Sharing Service Elevation of Privilege Vulnerability
CVE-2020-0689 - Microsoft Secure Boot Security Feature Bypass Vulnerability
CVE-2020-0698 - Windows Information Disclosure Vulnerability
CVE-2020-0703 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-0704 - Windows Wireless Network Manager Elevation of Privilege Vulnerability
CVE-2020-0705 - Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability
CVE-2020-0707 - Windows IME Elevation of Privilege Vulnerability
CVE-2020-0708 - Windows Imaging Library Remote Code Execution Vulnerability
CVE-2020-0709 - DirectX Elevation of Privilege Vulnerability
CVE-2020-0714 - DirectX Information Disclosure Vulnerability
CVE-2020-0715 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0716 - Win32k Information Disclosure Vulnerability
CVE-2020-0717 - Win32k Information Disclosure Vulnerability
CVE-2020-0719 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0720 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0721 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0722 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0723 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0724 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0725 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0726 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0731 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0732 - DirectX Elevation of Privilege Vulnerability
CVE-2020-0744 - Windows GDI Information Disclosure Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Malicious Software Removal Tool 64-bit
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows 10 Version 1803 for x64-based Systems
Windows 8.1 for x64-based systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems

Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft Surface Hub
Windows 10 Version 1709 for 32-bit Systems
Windows Malicious Software Removal Tool 32-bit
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1903 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Server, version 1909 (Server Core installation)
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0709
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0658
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0737
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0727

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0721
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0659
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0726
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0708
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0740
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0728
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0722
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0754
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0730
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0748
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0655
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0738
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0735
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0683
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0720
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0751
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0752
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0672
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0667
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0707
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0666
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0670
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0680
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0691

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0677
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0749
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0724
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0702
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0741
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0747
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0757
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0675
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0682
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0729
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0750
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0668
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0698
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0792
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0681
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0676
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0731
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0734
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0736
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0742
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0719
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0753
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0732
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0689

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0755
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0704
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0715
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0657
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0756
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0745
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0723
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0661
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0703
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0744
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0662
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0671
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0679
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0660
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0685
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0739
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0733
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0669
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0714
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0746
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0678
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0743
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0686
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0716

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0725
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0701
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0705
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0717
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0665
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0757
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0675
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0682
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0729
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0750
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0668
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0698
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0792
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0681
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0676
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0731
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0734
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0736

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0742
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0719
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0753
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0732
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0689
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0755
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0704
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0715
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0657
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0745
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0723
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0661
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0703
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0744
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0662

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0671
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0679
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0660
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0685
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0733
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0746
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0665
URL	https://support.microsoft.com/en-us/help/4537803
URL	https://support.microsoft.com/en-us/help/4502496
URL	https://support.microsoft.com/en-us/help/4537765
URL	https://support.microsoft.com/en-us/help/4537813
URL	https://support.microsoft.com/en-us/help/891716
URL	https://support.microsoft.com/en-us/help/4537822
URL	https://support.microsoft.com/en-us/help/4537794
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0756
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0737
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0658
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0705

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0709
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0717
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0725
URL	https://support.microsoft.com/en-us/help/4537814
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0716
URL	https://support.microsoft.com/en-us/help/4537776
URL	https://support.microsoft.com/en-us/help/4532693
URL	https://support.microsoft.com/en-us/help/4537764
URL	https://support.microsoft.com/en-us/help/4537789
URL	https://support.microsoft.com/en-us/help/4537762
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0686
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0743
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0678
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0714
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0669
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0739
URL	https://support.microsoft.com/en-us/help/4537820
URL	https://support.microsoft.com/en-us/help/4537821
URL	https://support.microsoft.com/en-us/help/4532691

Type	Reference
URL	https://support.microsoft.com/en-us/help/4537810
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0724
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0702
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0741
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0747
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0680
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0670
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0666
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0707
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0667
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0672
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0752
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0751
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0720
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0683
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0735

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0738
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0655
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0748
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0730
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0754
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0691
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0677
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0722
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0728
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0740
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0749
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0708
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0726
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0659
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0721
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0727

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0701

MS20-JAN: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their January 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-0640 - Internet Explorer Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2

Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0640
URL	https://support.microsoft.com/en-us/help/4534276
URL	https://support.microsoft.com/en-us/help/4534271
URL	https://support.microsoft.com/en-us/help/4534310
URL	https://support.microsoft.com/en-us/help/4534273
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0640
URL	https://support.microsoft.com/en-us/help/4534251
URL	https://support.microsoft.com/en-us/help/4528760
URL	https://support.microsoft.com/en-us/help/4534283
URL	https://support.microsoft.com/en-us/help/4534297
URL	https://support.microsoft.com/en-us/help/4534293
URL	https://support.microsoft.com/en-us/help/4534306
URL	https://support.microsoft.com/en-us/help/4534303

MS20-JAN: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their January 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-0601 - Windows CryptoAPI Spoofing Vulnerability
CVE-2020-0607 - Microsoft Graphics Components Information Disclosure Vulnerability
CVE-2020-0608 - Win32k Information Disclosure Vulnerability
CVE-2020-0609 - Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability
CVE-2020-0610 - Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability
CVE-2020-0611 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2020-0612 - Windows Remote Desktop Gateway (RD Gateway) Denial of Service Vulnerability
CVE-2020-0613 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0614 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0615 - Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2020-0616 - Microsoft Windows Denial of Service Vulnerability
CVE-2020-0617 - Hyper-V Denial of Service Vulnerability
CVE-2020-0636 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2020-0637 - Remote Desktop Web Access Information Disclosure Vulnerability
CVE-2020-0638 - Update Notification Manager Elevation of Privilege Vulnerability
CVE-2020-0639 - Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2020-0602 - ASP.NET Core Denial of Service Vulnerability
CVE-2020-0603 - ASP.NET Core Remote Code Execution Vulnerability
CVE-2020-0620 - Microsoft Cryptographic Services Elevation of Privilege Vulnerability
CVE-2020-0621 - Windows Security Feature Bypass Vulnerability
CVE-2020-0622 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-0623 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0624 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0625 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0626 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0627 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0628 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0629 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0630 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0631 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0632 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0633 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0634 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-0635 - Windows Elevation of Privilege Vulnerability
CVE-2020-0654 - Microsoft OneDrive for Android Security Feature Bypass Vulnerability
CVE-2020-0656 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-0641 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2020-0642 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0643 - Windows GDI+ Information Disclosure Vulnerability
CVE-2020-0644 - Windows Elevation of Privilege Vulnerability

Affected Products:
ASP.NET Core 2.1
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
ASP.NET Core 3.0

Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows Server 2019
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1803 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
ASP.NET Core 3.1
Dynamics 365 Field Service (on-premises) v7 series
Windows Server, version 1909 (Server Core installation)
One Drive for Android
Windows 10 Version 1909 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Windows 10 Version 1909 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0608
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0633
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0626
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0612
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0638
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0635
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0636
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0601
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0628
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0627
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0622
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0613
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0654
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0620
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0630
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0632
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0624
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0615
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0656
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0610
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0621
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0641
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0642

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0625
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0629
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0637
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0614
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0611
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0607
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0644
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0623
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0602
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0617
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0616
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0609
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0631
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0603
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0643
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0634
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0639
URL	https://support.microsoft.com/en-us/help/4534310
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0612
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0644
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0623
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0602

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0617
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0616
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0609
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0631
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0603
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0643
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0634
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0639
URL	https://support.microsoft.com/en-us/help/4534312
URL	https://support.microsoft.com/en-us/help/4534314
URL	https://support.microsoft.com/en-us/help/4534288
URL	https://support.microsoft.com/en-us/help/4534309
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0637
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0629
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0625
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0642
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0641

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0621
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0610
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0656
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0615
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0624
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0632
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0630
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0620
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0654
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0613
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0622
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0627
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0628
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0601
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0636
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0635

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0638
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0614
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0611
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0607
URL	https://support.microsoft.com/en-us/help/4534297
URL	https://support.microsoft.com/en-us/help/4534303
URL	https://support.microsoft.com/en-us/help/4534293
URL	https://support.microsoft.com/en-us/help/4534306
URL	https://support.microsoft.com/en-us/help/4534271
URL	https://support.microsoft.com/en-us/help/4534283
URL	https://support.microsoft.com/en-us/help/4528760
URL	https://support.microsoft.com/en-us/help/4534273
URL	https://support.microsoft.com/en-us/help/4534276
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0608
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0633
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0626

MS20-JUL: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their July 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-1403 - VBScript Remote Code Execution Vulnerability
CVE-2020-1416 - Visual Studio and Visual Studio Code Elevation of Privilege Vulnerability
CVE-2020-1432 - Skype for Business via Internet Explorer Information Disclosure Vulnerability

Affected Products:
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Microsoft Visual Studio 2019 version 16.6 (includes 16.0 - 16.5)
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Microsoft Visual Studio 2019 version 16.0
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Visual Studio Code
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Azure Storage Explorer
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for ARM64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
TypeScript

Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 2004 for 32-bit Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1432
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1403
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1416
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1416
URL	https://support.microsoft.com/en-us/help/4565524
URL	https://support.microsoft.com/en-us/help/4565513
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1432
URL	https://support.microsoft.com/en-us/help/4558998
URL	https://support.microsoft.com/en-us/help/4565541
URL	https://support.microsoft.com/en-us/help/4565511
URL	https://support.microsoft.com/en-us/help/4565503
URL	https://support.microsoft.com/en-us/help/4565508
URL	https://support.microsoft.com/en-us/help/4565479
URL	https://support.microsoft.com/en-us/help/4565537
URL	https://support.microsoft.com/en-us/help/4565536
URL	https://support.microsoft.com/en-us/help/4565489
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1403
URL	https://support.microsoft.com/en-us/help/4565483

MS20-JUL: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their July 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-1336 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1350 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2020-1418 - Windows Diagnostics Hub Elevation of Privilege Vulnerability
CVE-2020-1419 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1420 - Windows Error Reporting Information Disclosure Vulnerability
CVE-2020-1421 - LNK Remote Code Execution Vulnerability
CVE-2020-1422 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1423 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2020-1424 - Windows Update Stack Elevation of Privilege Vulnerability
ADV200008 - Microsoft Guidance for Enabling Request Smuggling Filter on IIS Servers
CVE-2020-1344 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1346 - Windows Modules Installer Elevation of Privilege Vulnerability
CVE-2020-1347 - Windows Storage Services Elevation of Privilege Vulnerability
CVE-2020-1351 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-1352 - Windows USO Core Worker Elevation of Privilege Vulnerability
CVE-2020-1353 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1354 - Windows UPnP Device Host Elevation of Privilege Vulnerability
CVE-2020-1355 - Windows Font Driver Host Remote Code Execution Vulnerability
CVE-2020-1356 - Windows iSCSI Target Service Elevation of Privilege Vulnerability
CVE-2020-1357 - Windows System Events Broker Elevation of Privilege Vulnerability
CVE-2020-1358 - Windows Resource Policy Information Disclosure Vulnerability
CVE-2020-1359 - Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
CVE-2020-1360 - Windows Profile Service Elevation of Privilege Vulnerability
CVE-2020-1361 - Windows WalletService Information Disclosure Vulnerability
CVE-2020-1362 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1363 - Windows Picker Platform Elevation of Privilege Vulnerability
CVE-2020-1364 - Windows WalletService Denial of Service Vulnerability
CVE-2020-1365 - Windows Event Logging Service Elevation of Privilege Vulnerability
CVE-2020-1366 - Windows Print Workflow Service Elevation of Privilege Vulnerability
CVE-2020-1367 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1368 - Windows Credential Enrollment Manager Service Elevation of Privilege Vulnerability
CVE-2020-1369 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1370 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1371 - Windows Event Logging Service Elevation of Privilege Vulnerability
CVE-2020-1372 - Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability

CVE-2020-1373 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1374 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2020-1375 - Windows COM Server Elevation of Privilege Vulnerability
CVE-2020-1381 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-1382 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-1384 - Windows CNG Key Isolation Service Elevation of Privilege Vulnerability
CVE-2020-1385 - Windows Credential Picker Elevation of Privilege Vulnerability
CVE-2020-1386 - Connected User Experiences and Telemetry Service Information Disclosure Vulnerability
CVE-2020-1387 - Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-1388 - Windows Elevation of Privilege Vulnerability
CVE-2020-1389 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1390 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1391 - Windows Agent Activation Runtime Information Disclosure Vulnerability
CVE-2020-1392 - Windows Elevation of Privilege Vulnerability
CVE-2020-1393 - Windows Diagnostics Hub Elevation of Privilege Vulnerability
CVE-2020-1394 - Windows Elevation of Privilege Vulnerability
CVE-2020-1395 - Windows Elevation of Privilege Vulnerability
CVE-2020-1396 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2020-1397 - Windows Imaging Component Information Disclosure Vulnerability
CVE-2020-1398 - Windows Lockscreen Elevation of Privilege Vulnerability
CVE-2020-1399 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1400 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1401 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1402 - Windows ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2020-1404 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1405 - Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability
CVE-2020-1406 - Windows Network List Service Elevation of Privilege Vulnerability
CVE-2020-1407 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1408 - Microsoft Graphics Remote Code Execution Vulnerability
CVE-2020-1410 - Windows Address Book Remote Code Execution Vulnerability
CVE-2020-1411 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1412 - Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1413 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1414 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1415 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1426 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1427 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1428 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1429 - Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2020-1430 - Windows UPnP Device Host Elevation of Privilege Vulnerability
CVE-2020-1431 - Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
CVE-2020-1434 - Windows Sync Host Service Elevation of Privilege Vulnerability
CVE-2020-1435 - GDI+ Remote Code Execution Vulnerability
CVE-2020-1436 - Windows Font Library Remote Code Execution Vulnerability
CVE-2020-1437 - Windows Network Location Awareness Service Elevation of Privilege Vulnerability
CVE-2020-1438 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1458 - Microsoft Office Remote Code Execution Vulnerability
CVE-2020-1461 - Microsoft Defender Elevation of Privilege Vulnerability

CVE-2020-1463 - Windows SharedStream Library Elevation of Privilege Vulnerability
CVE-2020-1465 - Microsoft OneDrive Elevation of Privilege Vulnerability
CVE-2020-1468 - Windows GDI Information Disclosure Vulnerability
CVE-2020-1469 - Bond Denial of Service Vulnerability
CVE-2020-1481 - Visual Studio Code ESLint Extention Remote Code Execution Vulnerability
CVE-2020-1032 - Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
CVE-2020-1036 - Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
CVE-2020-1040 - Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
CVE-2020-1041 - Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
CVE-2020-1043 - Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
CVE-2020-1240 - Microsoft Excel Remote Code Execution Vulnerability
CVE-2020-1249 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1267 - Local Security Authority Subsystem Service Denial of Service Vulnerability
CVE-2020-1333 - Group Policy Services Policy Processing Elevation of Privilege Vulnerability
CVE-2020-1042 - Hyper-V RemoteFX vGPU Remote Code Execution Vulnerability
CVE-2020-1085 - Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-1326 - Azure DevOps Server Cross-site Scripting Vulnerability
CVE-2020-1330 - Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Microsoft Visual Studio 2019 version 16.6 (includes 16.0 - 16.5)
Windows Defender on Windows Server 2019
Windows Defender on Windows Server 2012
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Microsoft 365 Apps for Enterprise for 64-bit Systems
Windows Defender on Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019
Windows Defender on Windows Server 2016 (Server Core installation)
Windows Defender on Windows Server, version 1803 (Server Core Installation)
Microsoft Visual Studio 2019 version 16.0
Microsoft System Center 2012 R2 Endpoint Protection
Windows Defender on Windows Server 2012 R2 (Server Core installation)
Windows Defender on Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows Defender on Windows 10 Version 1903 for x64-based Systems
Windows Defender on Windows Server 2016
Windows 8.1 for x64-based systems
Windows Defender on Windows 7 for 32-bit Systems Service Pack 1
OneDrive for Windows
Windows Defender on Windows 10 Version 1909 for 32-bit Systems

Windows 10 Version 1909 for x64-based Systems
Azure DevOps Server 2019 Update 1
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Azure DevOps Server 2019.0.1
Windows 10 Version 2004 for ARM64-based Systems
Microsoft Visual Studio 2015 Update 3
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Security Essentials
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Bond 9.0.1
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 1903 for ARM64-based Systems
Windows Defender on Windows 10 for 32-bit Systems
Windows Defender on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Defender on Windows 10 Version 1803 for x64-based Systems
Windows Defender on Windows 10 for x64-based Systems
Windows 10 Version 1809 for x64-based Systems
Microsoft System Center 2012 Endpoint Protection
Microsoft Forefront Endpoint Protection 2010
Windows Defender on Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1709 for ARM64-based Systems
Microsoft 365 Apps for Enterprise for 32-bit Systems
Windows Defender on Windows 10 Version 1903 for ARM64-based Systems
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Defender on Windows 10 Version 1803 for 32-bit Systems
Windows Defender on Windows 10 Version 1903 for 32-bit Systems
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Defender on Windows 10 Version 1607 for 32-bit Systems
Windows Defender on Windows 10 Version 1909 for ARM64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1607 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows 8.1 for x64-based systems

Windows Defender on Windows Server 2019 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Defender on Windows Server, version 1909 (Server Core installation)
Microsoft Visual Studio Code ESLint extension
Windows 10 Version 1909 for ARM64-based Systems
Windows Defender on Windows Server, version 1903 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows Defender on Windows 10 Version 1809 for 32-bit Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Defender on Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Defender on Windows Server 2012 R2
Windows 10 Version 1803 for ARM64-based Systems
Windows Defender on Windows 10 Version 1809 for ARM64-based Systems
Microsoft System Center Endpoint Protection
Windows Defender on Windows Server 2012 (Server Core installation)
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Azure DevOps Server 2019 Update 1.1
Windows Defender on Windows 7 for x64-based Systems Service Pack 1

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1344
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1424
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1036
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1436
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1032
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1346
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1412
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1401
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1418

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1368
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1422
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1330
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1369
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1375
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1387
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1371
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1434
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1423
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1352
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1042
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1400
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1386
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1430
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1362
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1382
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1350
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1394
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1404
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1384
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1437
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1421
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1040
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1413

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1415
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1397
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1363
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1267
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1431
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1385
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1468
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1393
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1410
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1043
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1355
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1372
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1398
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1326
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1240
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1366
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1357
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1353
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1374
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1041
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1435
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1426
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1336
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1419

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1395
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1458
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1391
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1359
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1465
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1396
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1481
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1405
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1414
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1361
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1333
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1381
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1367
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1354
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1469
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1390
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1461
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1427
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1358
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1408
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1365
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1429
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1420
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1406

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1402
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1411
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1463
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1347
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1360
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1356
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1438
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1249
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1392
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1407
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1399
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1388
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1373
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1370
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1389
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1085
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1428
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1364
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1351
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1426
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1435
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1041

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1353
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1395
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1419
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1336
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1458
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1391
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1374
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1357
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1359
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1344
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1465
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1396
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1481
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1405
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1414
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1361

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1333
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1381
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1366
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1326
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1240
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200008
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1355
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1372
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1398
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1043
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1410
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1393
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1431
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1363
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1040
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1421

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1437
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1404
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1394
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1350
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1382
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1362
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1430
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1386
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1352
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1367
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1354
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1469
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1390
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1427
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1461
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1358

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1408
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1365
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1420
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1429
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1406
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1402
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1400
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1434
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1423
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1371
URL	https://support.microsoft.com/en-us/help/4565552
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1411
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1463
URL	https://support.microsoft.com/en-us/help/4565911
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1347
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1360

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1356
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1438
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1392
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1249
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1388
URL	https://support.microsoft.com/en-us/help/4565540
URL	https://support.microsoft.com/en-us/help/4565912
URL	https://support.microsoft.com/en-us/help/4566785
URL	https://support.microsoft.com/en-us/help/4565529
URL	https://support.microsoft.com/en-us/help/4565553
URL	https://support.microsoft.com/en-us/help/4566425
URL	https://support.microsoft.com/en-us/help/4565354
URL	https://support.microsoft.com/en-us/help/4565535
URL	https://support.microsoft.com/en-us/help/4565353
URL	https://support.microsoft.com/en-us/help/4567703
URL	https://support.microsoft.com/en-us/help/4558997
URL	https://support.microsoft.com/en-us/help/4566426
URL	https://support.microsoft.com/en-us/help/4565539
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1399
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1407

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1373
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1370
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1389
URL	https://support.microsoft.com/en-us/help/4565554
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1085
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1428
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1364
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1351
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1424
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1036
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1385
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1468
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1267
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1397
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1415
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1384

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1413
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1042
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1387
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1369
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1375
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1422
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1330
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1368
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1418
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1401
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1412
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1346
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1436
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1032
URL	https://support.microsoft.com/en-us/help/4565511
URL	https://support.microsoft.com/en-us/help/4565536
URL	https://support.microsoft.com/en-us/help/4565524

Type	Reference
URL	https://support.microsoft.com/en-us/help/4565489
URL	https://support.microsoft.com/en-us/help/4565537
URL	https://support.microsoft.com/en-us/help/4565541
URL	https://support.microsoft.com/en-us/help/4558998
URL	https://support.microsoft.com/en-us/help/4565513
URL	https://support.microsoft.com/en-us/help/4565483
URL	https://support.microsoft.com/en-us/help/4565508
URL	https://support.microsoft.com/en-us/help/4565503

MS20-JUN: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their June 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-1213 - VBScript Remote Code Execution Vulnerability
CVE-2020-1214 - VBScript Remote Code Execution Vulnerability
CVE-2020-1215 - VBScript Remote Code Execution Vulnerability
CVE-2020-1216 - VBScript Remote Code Execution Vulnerability
CVE-2020-1219 - Microsoft Browser Memory Corruption Vulnerability
CVE-2020-1230 - VBScript Remote Code Execution Vulnerability
CVE-2020-1260 - VBScript Remote Code Execution Vulnerability
CVE-2020-1315 - Internet Explorer Information Disclosure Vulnerability

Affected Products:
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems

Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 2004 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1315
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1215
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1230
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1216
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1214
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1260
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1213
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1219
URL	https://support.microsoft.com/en-us/help/4561603
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1216
URL	https://support.microsoft.com/en-us/help/4561666
URL	https://support.microsoft.com/en-us/help/4561616
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1230
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1219
URL	https://support.microsoft.com/en-us/help/4561608
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1213
URL	https://support.microsoft.com/en-us/help/4561649

Type	Reference
URL	https://support.microsoft.com/en-us/help/4561643
URL	https://support.microsoft.com/en-us/help/4561670
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1315
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1215
URL	https://support.microsoft.com/en-us/help/4557957
URL	https://support.microsoft.com/en-us/help/4561612
URL	https://support.microsoft.com/en-us/help/4561621
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1214
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1260
URL	https://support.microsoft.com/en-us/help/4561602
URL	https://support.microsoft.com/en-us/help/4560960

MS20-JUN: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their June 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-0915 - Windows GDI Elevation of Privilege Vulnerability
CVE-2020-0916 - Windows GDI Elevation of Privilege Vulnerability
CVE-2020-0986 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1334 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1348 - Windows GDI Information Disclosure Vulnerability
CVE-2020-1196 - Windows Print Configuration Elevation of Privilege Vulnerability
CVE-2020-1197 - Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2020-1199 - Windows Feedback Hub Elevation of Privilege Vulnerability
CVE-2020-1201 - Windows Now Playing Session Manager Elevation of Privilege Vulnerability
CVE-2020-1202 - Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability

CVE-2020-1203 - Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1204 - Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability
CVE-2020-1206 - Windows SMBv3 Client/Server Information Disclosure Vulnerability
CVE-2020-1207 - Win32k Elevation of Privilege Vulnerability
CVE-2020-1208 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1209 - Windows Network List Service Elevation of Privilege Vulnerability
CVE-2020-1211 - Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2020-1212 - OLE Automation Elevation of Privilege Vulnerability
CVE-2020-1217 - Windows Runtime Information Disclosure Vulnerability
CVE-2020-1222 - Microsoft Store Runtime Elevation of Privilege Vulnerability
CVE-2020-1340 - NuGetGallery Spoofing Vulnerability
CVE-2020-1343 - Visual Studio Code Live Share Information Disclosure Vulnerability
CVE-2020-1120 - Connected User Experiences and Telemetry Service Denial of Service Vulnerability
CVE-2020-1194 - Windows Registry Denial of Service Vulnerability
CVE-2020-1231 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1232 - Media Foundation Information Disclosure Vulnerability
CVE-2020-1233 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1234 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-1235 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1236 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1237 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1238 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1239 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1246 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1247 - Win32k Elevation of Privilege Vulnerability
CVE-2020-1262 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1269 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1271 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-1274 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1275 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1277 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-1278 - Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1279 - Windows Lockscreen Elevation of Privilege Vulnerability
CVE-2020-1280 - Windows Bluetooth Service Elevation of Privilege Vulnerability
CVE-2020-1282 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1284 - Windows SMBv3 Client/Server Denial of Service Vulnerability
CVE-2020-1286 - Windows Shell Remote Code Execution Vulnerability
CVE-2020-1294 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1300 - Windows Remote Code Execution Vulnerability
CVE-2020-1307 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1310 - Win32k Elevation of Privilege Vulnerability
CVE-2020-1311 - Component Object Model Elevation of Privilege Vulnerability
CVE-2020-1312 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-1316 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1324 - Windows Elevation of Privilege Vulnerability
CVE-2020-1331 - System Center Operations Manager Spoofing Vulnerability
CVE-2020-1160 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-1162 - Windows Elevation of Privilege Vulnerability
CVE-2020-1163 - Microsoft Windows Defender Elevation of Privilege Vulnerability

CVE-2020-1170 - Microsoft Windows Defender Elevation of Privilege Vulnerability
CVE-2020-1241 - Windows Kernel Security Feature Bypass Vulnerability
CVE-2020-1244 - Connected User Experiences and Telemetry Service Denial of Service Vulnerability
CVE-2020-1248 - GDI+ Remote Code Execution Vulnerability
CVE-2020-1251 - Win32k Elevation of Privilege Vulnerability
CVE-2020-1253 - Win32k Elevation of Privilege Vulnerability
CVE-2020-1254 - Windows Modules Installer Service Elevation of Privilege Vulnerability
CVE-2020-1255 - Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability
CVE-2020-1257 - Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1258 - DirectX Elevation of Privilege Vulnerability
CVE-2020-1259 - Windows Host Guardian Service Security Feature Bypass Vulnerability
CVE-2020-1261 - Windows Error Reporting Information Disclosure Vulnerability
CVE-2020-1263 - Windows Error Reporting Information Disclosure Vulnerability
CVE-2020-1264 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1265 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1266 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1268 - Windows Service Information Disclosure Vulnerability
CVE-2020-1270 - Windows WLAN Service Elevation of Privilege Vulnerability
CVE-2020-1272 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-1273 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1276 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1281 - Windows OLE Remote Code Execution Vulnerability
CVE-2020-1283 - Windows Denial of Service Vulnerability
CVE-2020-1287 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-1290 - Win32k Information Disclosure Vulnerability
CVE-2020-1291 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-1292 - OpenSSH for Windows Elevation of Privilege Vulnerability
CVE-2020-1293 - Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1296 - Windows Diagnostics & feedback Information Disclosure Vulnerability
CVE-2020-1299 - LNK Remote Code Execution Vulnerability
CVE-2020-1301 - Windows SMB Remote Code Execution Vulnerability
CVE-2020-1302 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-1304 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1305 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1306 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1309 - Microsoft Store Runtime Elevation of Privilege Vulnerability
CVE-2020-1313 - Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-1314 - Windows Text Service Framework Elevation of Privilege Vulnerability
CVE-2020-1317 - Group Policy Elevation of Privilege Vulnerability
CVE-2020-1327 - Azure DevOps Server HTML Injection Vulnerability
CVE-2020-1329 - Microsoft Bing Search Spoofing Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Microsoft Visual Studio 2019 version 16.6 (includes 16.0 - 16.5)
Windows Defender on Windows Server 2019

Windows Defender on Windows Server 2012
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Defender on Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019
Windows Defender on Windows Server 2016 (Server Core installation)
Windows Defender on Windows Server, version 1803 (Server Core Installation)
Microsoft Visual Studio 2019 version 16.0
Microsoft System Center 2012 R2 Endpoint Protection
Windows Defender on Windows Server 2012 R2 (Server Core installation)
Windows Defender on Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows Defender on Windows 10 Version 1903 for x64-based Systems
Windows Defender on Windows Server 2016
Windows 8.1 for x64-based systems
Windows Defender on Windows 7 for 32-bit Systems Service Pack 1
System Center 2016 Operations Manager
Windows Defender on Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for x64-based Systems
Azure DevOps Server 2019 Update 1
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 2004 for HoloLens
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Azure DevOps Server 2019.0.1
Windows 10 Version 2004 for ARM64-based Systems
Microsoft Visual Studio 2015 Update 3
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Security Essentials
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
NuGetGallery
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 1903 for ARM64-based Systems
Windows Defender on Windows 10 for 32-bit Systems
Windows Defender on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Defender on Windows 10 Version 1803 for x64-based Systems

Windows Defender on Windows 10 for x64-based Systems
Windows 10 Version 1809 for HoloLens
Windows 10 Version 1809 for x64-based Systems
Microsoft System Center 2012 Endpoint Protection
Microsoft Forefront Endpoint Protection 2010
Windows Defender on Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1709 for ARM64-based Systems
Windows Defender on Windows 10 Version 1903 for ARM64-based Systems
Microsoft Visual Studio Code Live Share extension
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Defender on Windows 10 Version 1803 for 32-bit Systems
Windows Defender on Windows 10 Version 1903 for 32-bit Systems
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Defender on Windows 10 Version 1607 for 32-bit Systems
Windows Defender on Windows 10 Version 1909 for ARM64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows Defender on Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2
Microsoft Bing Search for Android
Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1607 for x64-based Systems
Windows Defender on Windows 10 Version 1709 for 32-bit Systems
Windows Defender on Windows 8.1 for x64-based systems
Windows Defender on Windows Server 2019 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows 10 Version 1903 for HoloLens
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Defender on Windows Server, version 1909 (Server Core installation)
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1909 for ARM64-based Systems
Windows Defender on Windows Server, version 1903 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows Defender on Windows 10 Version 1809 for 32-bit Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Server, version 1803 (Server Core Installation)
Windows Defender on Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Defender on Windows Server 2012 R2
Windows 10 Version 1803 for ARM64-based Systems
Windows Defender on Windows 10 Version 1809 for ARM64-based Systems
Microsoft System Center Endpoint Protection
Windows Defender on Windows Server 2012 (Server Core installation)

Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Azure DevOps Server 2019 Update 1.1
Windows Defender on Windows 7 for x64-based Systems Service Pack 1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1348
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0986
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1162
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1257
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1233
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1279
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1281
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1334
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1314
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1208
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1202
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1329
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1284
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1300
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1248
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1238
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1255
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1207

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1251
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1306
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1309
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1269
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1291
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1259
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1197
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1170
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1316
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1235
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1222
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1217
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1310
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1292
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1286
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1261
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1312
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1204
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1302
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1206
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1263
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1273
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0916
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1231

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1270
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1274
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1277
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1236
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1209
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1246
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1283
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1266
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1296
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1234
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1317
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1120
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1212
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1340
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1237
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1275
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1194
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1264
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1282
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1327
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1253
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1293
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1268
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1343

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1304
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1199
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1331
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1203
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1271
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1290
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1324
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1276
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1211
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1262
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1258
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1247
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1160
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1196
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1239
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1280
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1294
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1301
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1299
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1241
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1287
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1305
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1311
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1313

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1244
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1254
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1278
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1265
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1201
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1232
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0915
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1272
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1307
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1163
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0916
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1348
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1212
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1120
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1317
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1231
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1234
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1296
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1209

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1270
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1274
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1277
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1236
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1246
URL	https://support.microsoft.com/en-us/help/4557957
URL	https://support.microsoft.com/en-us/help/4562053
URL	https://support.microsoft.com/en-us/help/4566040
URL	https://support.microsoft.com/en-us/help/4561674
URL	https://support.microsoft.com/en-us/help/4561673
URL	https://support.microsoft.com/en-us/help/4561669
URL	https://support.microsoft.com/en-us/help/4561645
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1244
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1334
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1257
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1281
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1254
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1266

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1283
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1278
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0986
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1265
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1162
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1279
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1233
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1201
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1232
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0915
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1272
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1314
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1163
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1208
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1202
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1329

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1307
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1313
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1311
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1305
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1287
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1300
URL	https://support.microsoft.com/en-us/help/4549951
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1248
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1284
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1238
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1299
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1301
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1294
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1280
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1207
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1255

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1251
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1239
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1196
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1160
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1247
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1258
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1306
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1309
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1262
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1211
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1269
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1276
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1259
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1291
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1197
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1316

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1324
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1170
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1290
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1235
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1271
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1217
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1222
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1203
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1331
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1310
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1199
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1292
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1304
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1343
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1268
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1293

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1253
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1327
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1282
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1286
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1264
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1194
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1261
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1275
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1204
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1312
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1302
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1237
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1206
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1263
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1340
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1273

Type	Reference
URL	https://support.microsoft.com/en-us/help/4561612
URL	https://support.microsoft.com/en-us/help/4561621
URL	https://support.microsoft.com/en-us/help/4561602
URL	https://support.microsoft.com/en-us/help/4560960
URL	https://support.microsoft.com/en-us/help/4561608
URL	https://support.microsoft.com/en-us/help/4561649
URL	https://support.microsoft.com/en-us/help/4561643
URL	https://support.microsoft.com/en-us/help/4561670
URL	https://support.microsoft.com/en-us/help/4561666
URL	https://support.microsoft.com/en-us/help/4561616
URL	https://support.microsoft.com/en-us/help/4556799
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1241

MS20-MAR: Microsoft Internet Explorer Security Update High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-0768 - Scripting Engine Memory Corruption Vulnerability
CVE-2020-0824 - Internet Explorer Memory Corruption Vulnerability
CVE-2020-0830 - Scripting Engine Memory Corruption Vulnerability
CVE-2020-0832 - Scripting Engine Memory Corruption Vulnerability
CVE-2020-0833 - Scripting Engine Memory Corruption Vulnerability
CVE-2020-0847 - VBScript Remote Code Execution Vulnerability

Affected Products:
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems

Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2019
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2012

Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems

Solution Details

Microsoft has released a fix for this flaw in their March 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0832
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0830
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0824
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0833
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0847
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0768
URL	https://support.microsoft.com/en-us/help/4540671
URL	https://support.microsoft.com/en-us/help/4540689
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0830
URL	https://support.microsoft.com/en-us/help/4541506
URL	https://support.microsoft.com/en-us/help/4540673
URL	https://support.microsoft.com/en-us/help/4538461
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0832
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0847
URL	https://support.microsoft.com/en-us/help/4541510
URL	https://support.microsoft.com/en-us/help/4540670
URL	https://support.microsoft.com/en-us/help/4540693

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0833
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0824
URL	https://support.microsoft.com/en-us/help/4541509
URL	https://support.microsoft.com/en-us/help/4540688
URL	https://support.microsoft.com/en-us/help/4540681
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0768

MS20-MAR: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-0684 - LNK Remote Code Execution Vulnerability
CVE-2020-0700 - Azure DevOps Server Cross-site Scripting Vulnerability
CVE-2020-0758 - Azure DevOps Server and Team Foundation Services Elevation of Privilege Vulnerability
CVE-2020-0762 - Windows Defender Security Center Elevation of Privilege Vulnerability
CVE-2020-0763 - Windows Defender Security Center Elevation of Privilege Vulnerability
CVE-2020-0765 - Remote Desktop Connection Manager Information Disclosure Vulnerability
CVE-2020-0777 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0778 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-0779 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0780 - Windows Network List Service Elevation of Privilege Vulnerability
CVE-2020-0781 - Windows UPnP Service Elevation of Privilege Vulnerability
CVE-2020-0783 - Windows UPnP Service Elevation of Privilege Vulnerability
CVE-2020-0785 - Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2020-0786 - Windows Tile Object Service Denial of Service Vulnerability
CVE-2020-0787 - Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability
CVE-2020-0788 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0789 - Visual Studio Extension Installer Service Denial of Service Vulnerability
CVE-2020-0797 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0798 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0799 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-0800 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0801 - Media Foundation Memory Corruption Vulnerability
CVE-2020-0802 - Windows Network Connections Service Elevation of Privilege Vulnerability

CVE-2020-0803 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-0804 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-0806 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-0807 - Media Foundation Memory Corruption Vulnerability
CVE-2020-0808 - Provisioning Runtime Elevation of Privilege Vulnerability
CVE-2020-0809 - Media Foundation Memory Corruption Vulnerability
CVE-2020-0810 - Diagnostic Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-0814 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0815 - Azure DevOps Server and Team Foundation Services Elevation of Privilege Vulnerability
CVE-2020-0834 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2020-0840 - Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-0841 - Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-0842 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0843 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-0844 - Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-0845 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-0849 - Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-0853 - Windows Imaging Component Information Disclosure Vulnerability
CVE-2020-0854 - Windows Mobile Device Management Diagnostics Elevation of Privilege Vulnerability
CVE-2020-0872 - Remote Code Execution Vulnerability in Application Inspector
CVE-2020-0884 - Microsoft Visual Studio Spoofing Vulnerability
CVE-2020-0645 - Microsoft IIS Server Tampering Vulnerability
CVE-2020-0690 - DirectX Elevation of Privilege Vulnerability
CVE-2020-0769 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2020-0770 - Windows ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2020-0771 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2020-0772 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-0773 - Windows ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2020-0774 - Windows GDI Information Disclosure Vulnerability
CVE-2020-0775 - Windows Error Reporting Information Disclosure Vulnerability
CVE-2020-0776 - Windows Elevation of Privilege Vulnerability
CVE-2020-0791 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0793 - Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-0819 - Windows Device Setup Manager Elevation of Privilege Vulnerability
CVE-2020-0820 - Media Foundation Information Disclosure Vulnerability
CVE-2020-0822 - Windows Language Pack Installer Elevation of Privilege Vulnerability
CVE-2020-0857 - Windows Search Indexer Elevation of Privilege Vulnerability
CVE-2020-0858 - Windows Elevation of Privilege Vulnerability
CVE-2020-0859 - Windows Modules Installer Service Information Disclosure Vulnerability
CVE-2020-0860 - Windows ActiveX Installer Service Elevation of Privilege Vulnerability
CVE-2020-0861 - Windows Network Driver Interface Specification (NDIS) Information Disclosure Vulnerability
CVE-2020-0863 - Connected User Experiences and Telemetry Service Information Disclosure Vulnerability
CVE-2020-0864 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0865 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0866 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0867 - Windows Update Orchestrator Service Elevation of Privilege Vulnerability

CVE-2020-0868 - Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-0869 - Media Foundation Memory Corruption Vulnerability
CVE-2020-0871 - Windows Network Connections Service Information Disclosure Vulnerability
CVE-2020-0874 - Windows GDI Information Disclosure Vulnerability
CVE-2020-0876 - Win32k Information Disclosure Vulnerability
CVE-2020-0877 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0879 - Windows GDI Information Disclosure Vulnerability
CVE-2020-0880 - Windows GDI Information Disclosure Vulnerability
CVE-2020-0881 - GDI+ Remote Code Execution Vulnerability
CVE-2020-0882 - Windows GDI Information Disclosure Vulnerability
CVE-2020-0883 - GDI+ Remote Code Execution Vulnerability
CVE-2020-0885 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2020-0887 - Win32k Elevation of Privilege Vulnerability
CVE-2020-0896 - Windows Hard Link Elevation of Privilege Vulnerability
CVE-2020-0897 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2020-0898 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-0902 - Service Fabric Elevation of Privilege
CVE-2020-0905 - Dynamics Business Central Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Dynamics 365 Business Central 2019 Spring Update
Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
Windows 10 Version 1803 for x64-based Systems
Windows 8.1 for x64-based systems
Windows 10 Version 1909 for x64-based Systems
Azure DevOps Server 2019 Update 1
Windows 10 Version 1903 for 32-bit Systems
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)
Team Foundation Server 2018 Update 3.2
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Azure DevOps Server 2019.0.1
Service Fabric
Microsoft Visual Studio 2015 Update 3

Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1903 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Remote Desktop Connection Manager 2.7
Microsoft Dynamics 365 BC On Premise
Dynamics 365 Business Central 2019 Release Wave 2 (On-Premise)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Microsoft Dynamics NAV 2015
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Microsoft Dynamics NAV 2013
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Server, version 1909 (Server Core installation)
Team Foundation Server 2017 Update 3.1
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics NAV 2016
Microsoft Dynamics NAV 2018
Windows 10 Version 1709 for ARM64-based Systems
Microsoft Dynamics NAV 2017
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Windows 10 Version 1909 for 32-bit Systems
Team Foundation Server 2018 Update 1.2
Windows 10 Version 1803 for ARM64-based Systems
Application Inspector
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Azure DevOps Server 2019 Update 1.1

Solution Details

Microsoft has released a fix for this flaw in their March 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0840
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0700
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0874
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0876
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0771
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0861
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0684
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0849
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0841
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0845
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0762
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0802
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0781
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0822
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0774
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0860
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0772
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0854
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0787
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0779
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0879
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0804
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0797
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0815

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0690
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0645
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0806
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0789
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0763
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0868
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0819
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0807
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0800
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0863
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0758
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0902
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0857
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0778
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0864
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0871
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0786
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0885
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0867
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0898
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0791
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0881
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0788
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0882

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0887
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0843
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0869
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0820
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0799
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0858
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0834
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0872
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0853
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0809
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0810
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0844
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0783
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0814
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0785
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0770
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0769
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0775
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0801
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0776
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0877
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0884
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0777
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0793

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0798
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0896
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0765
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0803
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0865
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0897
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0808
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0880
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0866
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0905
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0780
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0773
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0842
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0883
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0859
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0822
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0841
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0774
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0860
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0762
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0849

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0771
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0876
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0874
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0700
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0840
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0859
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0883
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0684
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0842
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0773
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0780
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0905
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0866
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0880
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0808
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0897

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0865
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0803
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0765
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0896
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0798
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0793
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0777
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0884
URL	https://support.microsoft.com/en-us/help/4540681
URL	https://support.microsoft.com/en-us/help/4540688
URL	https://support.microsoft.com/en-us/help/4541509
URL	https://support.microsoft.com/en-us/help/4538461
URL	https://support.microsoft.com/en-us/help/4540673
URL	https://support.microsoft.com/en-us/help/4541506
URL	https://support.microsoft.com/en-us/help/4540670
URL	https://support.microsoft.com/en-us/help/4541510
URL	https://support.microsoft.com/en-us/help/4540693
URL	https://support.microsoft.com/en-us/help/4540689
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0861

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0877
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0776
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0801
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0775
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0769
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0770
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0785
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0814
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0783
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0844
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0810
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0809
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0853
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0872
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0834
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0858

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0799
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0820
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0869
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0843
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0887
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0882
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0788
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0881
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0791
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0898
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0867
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0885
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0786
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0871
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0864
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0778

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0857
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0902
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0758
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0863
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0800
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0807
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0819
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0781
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0802
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0868
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0763
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0845
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0789
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0806
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0645
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0690

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0815
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0797
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0804
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0879
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0779
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0787
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0854
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0772
URL	https://support.microsoft.com/en-us/help/4538886
URL	https://support.microsoft.com/en-us/help/4541500
URL	https://support.microsoft.com/en-us/help/4551258
URL	https://support.microsoft.com/en-us/help/4538888
URL	https://support.microsoft.com/en-us/help/4538032
URL	https://support.microsoft.com/en-us/help/4540694
URL	https://support.microsoft.com/en-us/help/4538887
URL	https://support.microsoft.com/en-us/help/4541505
URL	https://support.microsoft.com/en-us/help/4538708
URL	https://support.microsoft.com/en-us/help/4538884
URL	https://support.microsoft.com/en-us/help/4538885
URL	https://support.microsoft.com/en-us/help/4541504

Type	Reference
URL	https://support.microsoft.com/en-us/help/4551259

MS20-MAY: Microsoft Internet Explorer Security Update

High

Solution Details

Microsoft has released a fix for this flaw in their May 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-1035 - VBScript Remote Code Execution Vulnerability
CVE-2020-1058 - VBScript Remote Code Execution Vulnerability
CVE-2020-1060 - VBScript Remote Code Execution Vulnerability
CVE-2020-1062 - Internet Explorer Memory Corruption Vulnerability
CVE-2020-1064 - MSHTML Engine Remote Code Execution Vulnerability
CVE-2020-1093 - VBScript Remote Code Execution Vulnerability
CVE-2020-1092 - Internet Explorer Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2012

Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1060
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1093
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1064
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1035
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1092
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1062
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1058
URL	https://support.microsoft.com/en-us/help/4556798
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1060
URL	https://support.microsoft.com/en-us/help/4556826
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1035
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1064
URL	https://support.microsoft.com/en-us/help/4556860
URL	https://support.microsoft.com/en-us/help/4556807
URL	https://support.microsoft.com/en-us/help/4556812

Type	Reference
URL	https://support.microsoft.com/en-us/help/4556799
URL	https://support.microsoft.com/en-us/help/4556813
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1058
URL	https://support.microsoft.com/en-us/help/4551853
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1062
URL	https://support.microsoft.com/en-us/help/4556840
URL	https://support.microsoft.com/en-us/help/4556836
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1092
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1093
URL	https://support.microsoft.com/en-us/help/4556846

MS20-MAY: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-0909 - Windows Hyper-V Denial of Service Vulnerability
CVE-2020-1021 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-1028 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1192 - Visual Studio Code Python Extension Remote Code Execution Vulnerability
CVE-2020-0963 - Windows GDI Information Disclosure Vulnerability
CVE-2020-1010 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2020-1048 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-1054 - Win32k Elevation of Privilege Vulnerability
CVE-2020-1055 - Microsoft Active Directory Federation Services Cross-Site Scripting Vulnerability
CVE-2020-1061 - Microsoft Script Runtime Remote Code Execution Vulnerability
CVE-2020-1063 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-1071 - Windows Remote Access Common Dialog Elevation of Privilege Vulnerability
CVE-2020-1076 - Windows Denial of Service Vulnerability
CVE-2020-1078 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-1084 - Connected User Experiences and Telemetry Service Denial of Service Vulnerability
CVE-2020-1110 - Windows Update Stack Elevation of Privilege Vulnerability

CVE-2020-1113 - Windows Task Scheduler Security Feature Bypass Vulnerability
CVE-2020-1114 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1116 - Windows CSRSS Information Disclosure Vulnerability
CVE-2020-1118 - Microsoft Windows Transport Layer Security Denial of Service Vulnerability
CVE-2020-1124 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1126 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1134 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1135 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-1137 - Windows Push Notification Service Elevation of Privilege Vulnerability
CVE-2020-1138 - Windows Storage Service Elevation of Privilege Vulnerability
CVE-2020-1140 - DirectX Elevation of Privilege Vulnerability
CVE-2020-1143 - Win32k Elevation of Privilege Vulnerability
CVE-2020-1144 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1149 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1150 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1151 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1154 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-1155 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1156 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1157 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1158 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1175 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1179 - Windows GDI Information Disclosure Vulnerability
CVE-2020-1186 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1189 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1190 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1051 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1067 - Windows Remote Code Execution Vulnerability
CVE-2020-1068 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2020-1070 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-1072 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1075 - Windows Subsystem for Linux Information Disclosure Vulnerability
CVE-2020-1077 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1079 - Microsoft Windows Elevation of Privilege Vulnerability
CVE-2020-1081 - Windows Printer Service Elevation of Privilege Vulnerability
CVE-2020-1082 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-1086 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1087 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1088 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-1090 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1109 - Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-1111 - Windows Clipboard Service Elevation of Privilege Vulnerability
CVE-2020-1112 - Windows Background Intelligent Transfer Service Elevation of Privilege Vulnerability
CVE-2020-1117 - Microsoft Color Management Remote Code Execution Vulnerability
CVE-2020-1121 - Windows Clipboard Service Elevation of Privilege Vulnerability
CVE-2020-1123 - Connected User Experiences and Telemetry Service Denial of Service Vulnerability
CVE-2020-1125 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1131 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1132 - Windows Error Reporting Manager Elevation of Privilege Vulnerability

CVE-2020-1136 - Media Foundation Memory Corruption Vulnerability
CVE-2020-1139 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1141 - Windows GDI Information Disclosure Vulnerability
CVE-2020-1142 - Windows GDI Elevation of Privilege Vulnerability
CVE-2020-1145 - Windows GDI Information Disclosure Vulnerability
CVE-2020-1153 - Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1161 - ASP.NET Core Denial of Service Vulnerability
CVE-2020-1164 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1165 - Windows Clipboard Service Elevation of Privilege Vulnerability
CVE-2020-1166 - Windows Clipboard Service Elevation of Privilege Vulnerability
CVE-2020-1171 - Visual Studio Code Python Extension Remote Code Execution Vulnerability
CVE-2020-1173 - Microsoft Power BI Report Server Spoofing Vulnerability
CVE-2020-1174 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1176 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1184 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1185 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1187 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1188 - Windows State Repository Service Elevation of Privilege Vulnerability
CVE-2020-1191 - Windows State Repository Service Elevation of Privilege Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
Windows 10 Version 1803 for x64-based Systems
Windows 8.1 for x64-based systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Microsoft Visual Studio 2017 version 15.9 (includes 15.1 - 15.8)
Windows 10 Version 1803 for 32-bit Systems
Microsoft Dynamics 365 (on-premises) version 8.2
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1903 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems

Microsoft Visual Studio 2019 version 16.5
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
ASP.NET Core 3.1
Windows Server, version 1909 (Server Core installation)
Power BI Report Server
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server, version 1803 (Server Core Installation)
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their May 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 9.9

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1077
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1110
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1150
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1185
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1078
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1021

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1141
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1179
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1054
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1149
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1131
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1151
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1121
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1135
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1118
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1140
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1175
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1079
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1082
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1051
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1090
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1068
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1028
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1010
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1111
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1084
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1189
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1174
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1156
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1157

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1063
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1075
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0909
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1125
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1116
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1088
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1184
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1067
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1081
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1142
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1126
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1158
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1161
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1136
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1154
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1109
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1176
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1138
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1186
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0963
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1191
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1072
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1137

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1190
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1048
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1187
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1134
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1143
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1192
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1070
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1164
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1188
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1166
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1114
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1076
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1123
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1155
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1165
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1139
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1055
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1112
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1171
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1113
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1086
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1087
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1153
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1173

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1071
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1132
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1061
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1117
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1144
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1124
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1141
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1157
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1156
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1150
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1079
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1188
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1151
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1175
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1144
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1113
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1067
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1191

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1186
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1171
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0963
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1112
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1134
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1121
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1139
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1082
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1135
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1137
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1190
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1165
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1187
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1164
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1068
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1124

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1070
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1061
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1140
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1184
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1010
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1145
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1055
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1076
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1114
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1174
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1189
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1136
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1084
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1158
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1149
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1051

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1072
URL	https://support.microsoft.com/en-us/help/4551998
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1166
URL	https://support.microsoft.com/en-us/help/4556853
URL	https://support.microsoft.com/en-us/help/4556854
URL	https://support.microsoft.com/en-us/help/4556836
URL	https://support.microsoft.com/en-us/help/4556813
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1173
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1143
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1126
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1132
URL	https://support.microsoft.com/en-us/help/4556807
URL	https://support.microsoft.com/en-us/help/4551853
URL	https://support.microsoft.com/en-us/help/4556812
URL	https://support.microsoft.com/en-us/help/4556860
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1192
URL	https://support.microsoft.com/en-us/help/4556799
URL	https://support.microsoft.com/en-us/help/4556846
URL	https://support.microsoft.com/en-us/help/4556840
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1028

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1077
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1088
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1111
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1087
URL	https://support.microsoft.com/en-us/help/4556826
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1109
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1179
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1086
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1118
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1090
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1110
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1048
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1075
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1125
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1161
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0909

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1063
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1154
URL	https://support.microsoft.com/en-us/help/4556852
URL	https://support.microsoft.com/en-us/help/4552002
URL	https://support.microsoft.com/en-us/help/4556843
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1131
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1054
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1123
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1116
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1185
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1155
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1078
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1021
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1071
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1081
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1142
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1153

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1117
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1138
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1176

MS20-NOV: Microsoft Internet Explorer Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-17052 - Scripting Engine Memory Corruption Vulnerability
CVE-2020-17053 - Internet Explorer Memory Corruption Vulnerability
CVE-2020-17058 - Microsoft Browser Memory Corruption Vulnerability

Affected Products:
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 20H2 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

Internet Explorer 11 on Windows 10 Version 2004 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 20H2 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows Server 2012
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 2004 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 20H2 for 32-bit Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their November 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.1

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17058
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17053
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17052

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17058
URL	https://support.microsoft.com/en-us/help/4586834
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17053
URL	https://support.microsoft.com/en-us/help/4586845
URL	https://support.microsoft.com/en-us/help/4586827
URL	https://support.microsoft.com/en-us/help/4586787
URL	https://support.microsoft.com/en-us/help/4586786
URL	https://support.microsoft.com/en-us/help/4586785
URL	https://support.microsoft.com/en-us/help/4586781
URL	https://support.microsoft.com/en-us/help/4586768
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17052
URL	https://support.microsoft.com/en-us/help/4586793
URL	https://support.microsoft.com/en-us/help/4586830

MS20-NOV: Microsoft Windows Security Update High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their November 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-16970 - Azure Sphere Unsigned Code Execution Vulnerability
CVE-2020-16997 - Remote Desktop Protocol Server Information Disclosure Vulnerability
CVE-2020-16998 - DirectX Elevation of Privilege Vulnerability

CVE-2020-16999 - Windows WalletService Information Disclosure Vulnerability
CVE-2020-17000 - Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2020-17001 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-17004 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2020-17055 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17056 - Windows Network File System Information Disclosure Vulnerability
CVE-2020-17057 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2020-17068 - Windows GDI+ Remote Code Execution Vulnerability
CVE-2020-17069 - Windows NDIS Information Disclosure Vulnerability
CVE-2020-17070 - Windows Update Medic Service Elevation of Privilege Vulnerability
CVE-2020-17071 - Windows Delivery Optimization Information Disclosure Vulnerability
CVE-2020-17073 - Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-17074 - Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-17075 - Windows USO Core Worker Elevation of Privilege Vulnerability
CVE-2020-17076 - Windows Update Orchestrator Service Elevation of Privilege Vulnerability
CVE-2020-17077 - Windows Update Stack Elevation of Privilege Vulnerability
CVE-2020-17078 - Raw Image Extension Remote Code Execution Vulnerability
CVE-2020-17079 - Raw Image Extension Remote Code Execution Vulnerability
CVE-2020-17087 - Windows Kernel Local Elevation of Privilege Vulnerability
CVE-2020-17088 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-17090 - Microsoft Defender for Endpoint Security Feature Bypass Vulnerability
CVE-2020-17091 - Microsoft Teams Remote Code Execution Vulnerability
CVE-2020-17100 - Visual Studio Tampering Vulnerability
CVE-2020-17101 - HEIF Image Extensions Remote Code Execution Vulnerability
CVE-2020-17102 - WebP Image Extensions Information Disclosure Vulnerability
CVE-2020-17105 - AV1 Video Extension Remote Code Execution Vulnerability
CVE-2020-17106 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2020-17107 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2020-17108 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2020-17109 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2020-17110 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2020-17113 - Windows Camera Codec Information Disclosure Vulnerability
CVE-2020-1599 - Windows Spoofing Vulnerability
CVE-2020-16981 - Azure Sphere Elevation of Privilege Vulnerability
CVE-2020-16982 - Azure Sphere Unsigned Code Execution Vulnerability
CVE-2020-16983 - Azure Sphere Tampering Vulnerability
CVE-2020-16984 - Azure Sphere Unsigned Code Execution Vulnerability
CVE-2020-16985 - Azure Sphere Information Disclosure Vulnerability
CVE-2020-16986 - Azure Sphere Denial of Service Vulnerability
CVE-2020-16987 - Azure Sphere Unsigned Code Execution Vulnerability
CVE-2020-16988 - Azure Sphere Elevation of Privilege Vulnerability
CVE-2020-16989 - Azure Sphere Elevation of Privilege Vulnerability
CVE-2020-16990 - Azure Sphere Information Disclosure Vulnerability
CVE-2020-16991 - Azure Sphere Unsigned Code Execution Vulnerability
CVE-2020-16992 - Azure Sphere Elevation of Privilege Vulnerability
CVE-2020-16993 - Azure Sphere Elevation of Privilege Vulnerability
CVE-2020-16994 - Azure Sphere Unsigned Code Execution Vulnerability
CVE-2020-17005 - Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability
CVE-2020-17006 - Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability

CVE-2020-17007 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-17010 - Win32k Elevation of Privilege Vulnerability
CVE-2020-17011 - Windows Port Class Library Elevation of Privilege Vulnerability
CVE-2020-17012 - Windows Bind Filter Driver Elevation of Privilege Vulnerability
CVE-2020-17013 - Win32k Information Disclosure Vulnerability
CVE-2020-17014 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-17018 - Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability
CVE-2020-17021 - Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability
CVE-2020-17024 - Windows Client Side Rendering Print Provider Elevation of Privilege Vulnerability
CVE-2020-17025 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17026 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17027 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17028 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17029 - Windows Canonical Display Driver Information Disclosure Vulnerability
CVE-2020-17030 - Windows MSCTF Server Information Disclosure Vulnerability
CVE-2020-17031 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17032 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17033 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17034 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17035 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-17036 - Windows Function Discovery SSDP Provider Information Disclosure Vulnerability
CVE-2020-17037 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2020-17038 - Win32k Elevation of Privilege Vulnerability
CVE-2020-17040 - Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2020-17041 - Windows Print Configuration Elevation of Privilege Vulnerability
CVE-2020-17042 - Windows Print Spooler Remote Code Execution Vulnerability
CVE-2020-17043 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17044 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2020-17045 - Windows KernelStream Information Disclosure Vulnerability
CVE-2020-17046 - Windows Error Reporting Denial of Service Vulnerability
CVE-2020-17047 - Windows Network File System Denial of Service Vulnerability
CVE-2020-17049 - Kerberos Security Feature Bypass Vulnerability
CVE-2020-17051 - Windows Network File System Remote Code Execution Vulnerability
CVE-2020-17081 - Microsoft Raw Image Extension Information Disclosure Vulnerability
CVE-2020-17082 - Raw Image Extension Remote Code Execution Vulnerability
CVE-2020-17086 - Raw Image Extension Remote Code Execution Vulnerability
CVE-2020-17104 - Visual Studio Code JSHint Extension Remote Code Execution Vulnerability
CVE-2020-1325 - Azure DevOps Server and Team Foundation Services Spoofing Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
HEIF Image Extension
HEVC Video Extensions
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)

Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
Windows 10 Version 1803 for x64-based Systems
Raw Image Extension
Windows 8.1 for x64-based systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1803 for 32-bit Systems
WebP Image Extension
Microsoft Dynamics 365 (on-premises) version 8.2
Windows 10 Version 1903 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 2004 for ARM64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 1903 for ARM64-based Systems
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Azure Sphere
Windows 10 Version 1809 for x64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Server, version 1909 (Server Core installation)
Microsoft Dynamics CRM 2015 (on-premises) version 7.0
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
AV1 Video Extension
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Microsoft Visual Studio 2019 version 16.8
Windows Server 2019 (Server Core installation)

Windows Server 2016
Microsoft Teams
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Azure DevOps Server 2019 Update 1.1

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17074
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17030
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17034
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16991
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17082
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17007
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17057
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1325
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16992
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16999
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1599
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16989
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17004
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17042
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17088
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17046
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17031
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17038
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16985
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17032

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17109
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17047
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17043
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17091
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17073
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17106
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17110
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17105
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17045
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17010
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16998
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17044
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17018
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17100
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17102
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17012
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17079
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16982
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17087
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17005
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17070
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16986
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17090
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17104

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17055
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17068
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16990
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17037
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17036
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17024
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17086
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17040
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17051
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17069
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17025
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16981
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17056
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17113
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17078
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17107
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17027
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17108
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17035
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17077
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16970
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17028
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17041
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17026

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16994
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16993
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17033
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17075
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16984
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17006
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17029
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17000
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17071
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17021
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17076
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16997
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17013
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17011
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16983
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17001
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17101
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17049
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16988
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17081
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16987
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17014
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16985

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17038
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17031
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17046
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17004
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17088
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17042
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16989
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1599
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16999
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16992
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1325
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17057
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17007
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17082
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16991
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17034

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17030
URL	https://support.microsoft.com/en-us/help/4586834
URL	https://support.microsoft.com/en-us/help/4586793
URL	https://support.microsoft.com/en-us/help/4586830
URL	https://support.microsoft.com/en-us/help/4586781
URL	https://support.microsoft.com/en-us/help/4586786
URL	https://support.microsoft.com/en-us/help/4586787
URL	https://support.microsoft.com/en-us/help/4586845
URL	https://support.microsoft.com/en-us/help/4586827
URL	https://support.microsoft.com/en-us/help/4586785
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17032
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17047
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17109
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17043
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17091
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17073
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17106
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17110
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17074

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17045
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17010
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17105
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17044
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16998
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17018
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17100
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17012
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17102
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17079
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16982
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17005
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17087
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17070
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16986
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17090

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17104
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17055
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17068
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16990
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17037
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17036
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17024
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17086
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17040
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17051
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17069
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17025
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16981
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17056
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17113
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17078

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17107
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17027
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17035
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17108
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16970
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17077
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17041
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17028
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17026
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16994
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16993
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17033
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17075
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16984
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17029
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17006

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17000
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17071
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17076
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17021
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16997
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17011
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17013
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16983
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17001
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17101
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17049
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16988
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17081
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16987
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17014
URL	https://support.microsoft.com/en-us/help/4586808

Type	Reference
URL	https://support.microsoft.com/en-us/help/4584611
URL	https://support.microsoft.com/en-us/help/4586805
URL	https://support.microsoft.com/en-us/help/4584612
URL	https://support.microsoft.com/en-us/help/4577009
URL	https://support.microsoft.com/en-us/help/4586807
URL	https://support.microsoft.com/en-us/help/4586817
URL	https://support.microsoft.com/en-us/help/4586823

MS20-NOV: Microsoft Windows Security Update - Registry Entry Not Set

High

Vulnerability Details

A security feature bypass vulnerability exists in the way Key Distribution Center (KDC) determines if a service ticket can be used for delegation via Kerberos Constrained Delegation (KCD). To exploit the vulnerability, a compromised service that is configured to use KCD could tamper with a service ticket that is not valid for delegation to force the KDC to accept it.

The Microsoft patch for this vulnerability has already been installed, however, the scanner has detected the registry changes required to fully remediate this vulnerability have not been set.
Impact:
An attacker could exploit this vulnerability to impersonate authenticated users or obtain Kerberos service tickets without proper authorization.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

The MS20-NOV patch has already been applied. By default, Windows servers have full mitigation for this vulnerability disabled. In order to fully remediate this vulnerability, a registry entry needs to be added.

Microsoft advises waiting at least a week to allow all outstanding Service for User to Self (S4U2self) Kerberos service tickets to expire. Then full protection can be enabled by adding the following registry key to enable Active Directory domain controller Enforcement mode .

Key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Kdc
Value: PerformTicketSignature = 2
Value Type: DWORD (Decimal value)

Note that Windows Server 2008 SP2 and Windows Server 2008 R2 require the MS20-DEC patch to be installed as well.

CVSS Base Score: 7.2

CVSS Vector: AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17049
URL	https://support.microsoft.com/en-us/help/4598347/managing-deployment-of-kerberos-s4u-changes-for-cve
URL	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2020-17049

MS20-OCT: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their October 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-16863 - Windows Remote Desktop Service Denial of Service Vulnerability
CVE-2020-16876 - Windows Application Compatibility Client Library Elevation of Privilege Vulnerability
CVE-2020-16877 - Windows Elevation of Privilege Vulnerability
CVE-2020-16889 - Windows KernelStream Information Disclosure Vulnerability
CVE-2020-16890 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-16891 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2020-16892 - Windows Image Elevation of Privilege Vulnerability
CVE-2020-16894 - Windows NAT Remote Code Execution Vulnerability
CVE-2020-16895 - Windows Error Reporting Manager Elevation of Privilege Vulnerability
CVE-2020-16896 - Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
CVE-2020-16897 - NetBT Information Disclosure Vulnerability
CVE-2020-16904 - Azure Functions Elevation of Privilege Vulnerability
CVE-2020-16918 - Base3D Remote Code Execution Vulnerability
CVE-2020-16919 - Windows Enterprise App Management Service Information Disclosure Vulnerability
CVE-2020-16920 - Windows Application Compatibility Client Library Elevation of Privilege Vulnerability
CVE-2020-16921 - Windows Text Services Framework Information Disclosure Vulnerability
CVE-2020-16922 - Windows Spoofing Vulnerability
CVE-2020-16923 - Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-16924 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-16927 - Windows Remote Desktop Protocol (RDP) Denial of Service Vulnerability
CVE-2020-16935 - Windows COM Server Elevation of Privilege Vulnerability

CVE-2020-16938 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-16976 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16977 - Visual Studio Code Python Extension Remote Code Execution Vulnerability
CVE-2020-16995 - Network Watcher Agent Virtual Machine Extension for Linux Elevation of Privilege Vulnerability
CVE-2020-17003 - Base3D Remote Code Execution Vulnerability
CVE-2020-0764 - Windows Storage Services Elevation of Privilege Vulnerability
CVE-2020-1047 - Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2020-1080 - Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2020-1167 - Microsoft Graphics Components Remote Code Execution Vulnerability
CVE-2020-1243 - Windows Hyper-V Denial of Service Vulnerability
CVE-2020-16885 - Windows Storage VSP Driver Elevation of Privilege Vulnerability
CVE-2020-16886 - PowerShellGet Module WDAC Security Feature Bypass Vulnerability
CVE-2020-16887 - Windows Network Connections Service Elevation of Privilege Vulnerability
CVE-2020-16898 - Windows TCP/IP Remote Code Execution Vulnerability
CVE-2020-16899 - Windows TCP/IP Denial of Service Vulnerability
CVE-2020-16900 - Windows Event System Elevation of Privilege Vulnerability
CVE-2020-16901 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-16902 - Windows Installer Elevation of Privilege Vulnerability
CVE-2020-16905 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-16907 - Win32k Elevation of Privilege Vulnerability
CVE-2020-16908 - Windows Setup Elevation of Privilege Vulnerability
CVE-2020-16909 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2020-16910 - Windows Security Feature Bypass Vulnerability
CVE-2020-16911 - GDI+ Remote Code Execution Vulnerability
CVE-2020-16912 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16913 - Win32k Elevation of Privilege Vulnerability
CVE-2020-16914 - Windows GDI+ Information Disclosure Vulnerability
CVE-2020-16915 - Media Foundation Memory Corruption Vulnerability
CVE-2020-16916 - Windows COM Server Elevation of Privilege Vulnerability
CVE-2020-16936 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16939 - Group Policy Elevation of Privilege Vulnerability
CVE-2020-16940 - Windows - User Profile Service Elevation of Privilege Vulnerability
CVE-2020-16943 - Dynamics 365 Commerce Elevation of Privilege Vulnerability
CVE-2020-16956 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-16967 - Windows Camera Codec Pack Remote Code Execution Vulnerability
CVE-2020-16968 - Windows Camera Codec Pack Remote Code Execution Vulnerability
CVE-2020-16972 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16973 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16974 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16975 - Windows Backup Service Elevation of Privilege Vulnerability
CVE-2020-16978 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-16980 - Windows iSCSI Target Service Elevation of Privilege Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems

Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft 365 Apps for Enterprise for 32-bit Systems
Windows Server 2012 (Server Core installation)
Microsoft 365 Apps for Enterprise for 64-bit Systems
Windows Server 2012
Windows Server 2019
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Windows 10 Version 1803 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Server, version 1909 (Server Core installation)
Dynamics 365 Commerce
Azure Functions
Windows 10 Version 1909 for x64-based Systems
PowerShellGet 2.2.5
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Windows 10 Version 1803 for 32-bit Systems
Network Watcher Agent virtual machine extension for Linux
Microsoft Dynamics 365 (on-premises) version 8.2
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1709 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 1903 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016

Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
3D Viewer

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16940
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16924
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16918
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16894
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16975
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16956
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16939
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16876
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16904
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-17003
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16977
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16895
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16905
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16935
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16976
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16978
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16899
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16889
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16927

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16915
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16898
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16916
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16877
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16896
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16897
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16936
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16973
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16919
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16921
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16900
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16974
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16863
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16901
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1080
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0764
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16923
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16943
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16914
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1047
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16907
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16887
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16902
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16972

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16913
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16938
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1243
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16911
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16922
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16912
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16920
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16980
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16995
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16908
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16910
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16891
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1167
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16968
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16909
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16967
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16886
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16885
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16890
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16892
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16877
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16891
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16897

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16924
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16936
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16898
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16919
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1167
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16921
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16900
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16973
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16968
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16974
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16909
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16890
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16885
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16886
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16967
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16863

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0764
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1080
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16901
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16923
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16892
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16943
URL	https://support.microsoft.com/en-us/help/4577041
URL	https://support.microsoft.com/en-us/help/4577049
URL	https://support.microsoft.com/en-us/help/4580353
URL	https://support.microsoft.com/en-us/help/4580330
URL	https://support.microsoft.com/en-us/help/4577671
URL	https://support.microsoft.com/en-us/help/4580378
URL	https://support.microsoft.com/en-us/help/4580358
URL	https://support.microsoft.com/en-us/help/4580327
URL	https://support.microsoft.com/en-us/help/4580385
URL	https://support.microsoft.com/en-us/help/4580328
URL	https://support.microsoft.com/en-us/help/4577668
URL	https://support.microsoft.com/en-us/help/4580382
URL	https://support.microsoft.com/en-us/help/4580347
URL	https://support.microsoft.com/en-us/help/4580387
URL	https://support.microsoft.com/en-us/help/4578106

Type	Reference
URL	https://support.microsoft.com/en-us/help/4580345
URL	https://support.microsoft.com/en-us/help/4580346
URL	https://support.microsoft.com/en-us/help/4579311
URL	https://support.microsoft.com/en-us/help/4578105
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16914
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16918
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16894
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1047
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16975
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16907
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16887
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16902
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16972
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16938
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16913
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16956
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1243

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16939
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16876
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16911
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16922
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16916
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16910
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16978
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16915
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16908
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16927
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16889
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16899
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16995
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16940
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16976
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16935

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16980
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16905
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16895
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16977
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17003
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16920
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16904
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16912
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16896

MS20-SEP: Microsoft Internet Explorer Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2020-1506 - Windows Start-Up Application Elevation of Privilege Vulnerability
CVE-2020-0878 - Microsoft Browser Memory Corruption Vulnerability
CVE-2020-1012 - WinINet API Elevation of Privilege Vulnerability

Affected Products:
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems

Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems
ChakraCore
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1903 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 2004 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2019
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2012
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 2004 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their September 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1506
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0878
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1012
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1506
URL	https://support.microsoft.com/en-us/help/4577038
URL	https://support.microsoft.com/en-us/help/4577051
URL	https://support.microsoft.com/en-us/help/4571756
URL	https://support.microsoft.com/en-us/help/4574727
URL	https://support.microsoft.com/en-us/help/4570333
URL	https://support.microsoft.com/en-us/help/4577032
URL	https://support.microsoft.com/en-us/help/4577041
URL	https://support.microsoft.com/en-us/help/4577049
URL	https://support.microsoft.com/en-us/help/4577010
URL	https://support.microsoft.com/en-us/help/4577015
URL	https://support.microsoft.com/en-us/help/4577066
URL	https://support.microsoft.com/en-us/help/4577064

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0878
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1012

MS20-SEP: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their September 2020 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-1532 - Windows InstallService Elevation of Privilege Vulnerability
CVE-2020-16856 - Visual Studio Remote Code Execution Vulnerability
CVE-2020-16857 - Microsoft Dynamics 365 for Finance and Operations (on-premises) Remote Code Execution Vulnerability
CVE-2020-16858 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-16859 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-16860 - Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability
CVE-2020-16861 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-16862 - Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability
CVE-2020-16864 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-16872 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-16878 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-16879 - Projected Filesystem Information Disclosure Vulnerability
CVE-2020-16881 - Visual Studio JSON Remote Code Execution Vulnerability
CVE-2020-1376 - Windows Elevation of Privilege Vulnerability
CVE-2020-1471 - Windows CloudExperienceHost Elevation of Privilege Vulnerability
CVE-2020-1491 - Windows Function Discovery Service Elevation of Privilege Vulnerability
CVE-2020-1507 - Microsoft COM for Windows Elevation of Privilege Vulnerability
CVE-2020-1508 - Windows Media Audio Decoder Remote Code Execution Vulnerability
CVE-2020-1559 - Windows Storage Services Elevation of Privilege Vulnerability
CVE-2020-1589 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1590 - Connected User Experiences and Telemetry Service Elevation of Privilege Vulnerability
CVE-2020-1592 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1593 - Windows Media Audio Decoder Remote Code Execution Vulnerability
CVE-2020-1596 - TLS Information Disclosure Vulnerability

CVE-2020-1598 - Windows UPnP Service Elevation of Privilege Vulnerability
CVE-2020-0648 - Windows RSoP Service Application Elevation of Privilege Vulnerability
CVE-2020-0664 - Active Directory Information Disclosure Vulnerability
CVE-2020-0718 - Active Directory Remote Code Execution Vulnerability
CVE-2020-0761 - Active Directory Remote Code Execution Vulnerability
CVE-2020-0766 - Microsoft Store Runtime Elevation of Privilege Vulnerability
CVE-2020-0782 - Windows Cryptographic Catalog Services Elevation of Privilege Vulnerability
CVE-2020-0790 - Microsoft splwow64 Elevation of Privilege Vulnerability
CVE-2020-0805 - Projected Filesystem Security Feature Bypass Vulnerability
CVE-2020-0836 - Windows DNS Denial of Service Vulnerability
CVE-2020-0837 - ADFS Spoofing Vulnerability
CVE-2020-0838 - NTFS Elevation of Privilege Vulnerability
CVE-2020-0839 - Windows dnsrslvr.dll Elevation of Privilege Vulnerability
CVE-2020-0856 - Active Directory Information Disclosure Vulnerability
CVE-2020-0870 - Shell infrastructure component Elevation of Privilege Vulnerability
CVE-2020-0875 - Microsoft splwow64 Information Disclosure Vulnerability
CVE-2020-0886 - Windows Storage Services Elevation of Privilege Vulnerability
CVE-2020-0890 - Windows Hyper-V Denial of Service Vulnerability
CVE-2020-0904 - Windows Hyper-V Denial of Service Vulnerability
CVE-2020-0908 - Windows Text Service Module Remote Code Execution Vulnerability
CVE-2020-0911 - Windows Modules Installer Elevation of Privilege Vulnerability
CVE-2020-0912 - Windows Function Discovery SSDP Provider Elevation of Privilege Vulnerability
CVE-2020-0914 - Windows State Repository Service Information Disclosure Vulnerability
CVE-2020-0921 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-0922 - Microsoft COM for Windows Remote Code Execution Vulnerability
CVE-2020-0928 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-0941 - Win32k Information Disclosure Vulnerability
CVE-2020-0951 - Windows Defender Application Control Security Feature Bypass Vulnerability
CVE-2020-0989 - Windows Mobile Device Management Diagnostics Information Disclosure Vulnerability
CVE-2020-0997 - Windows Camera Codec Pack Remote Code Execution Vulnerability
CVE-2020-0998 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2020-1013 - Group Policy Elevation of Privilege Vulnerability
CVE-2020-1030 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2020-1031 - Windows DHCP Server Information Disclosure Vulnerability
CVE-2020-1033 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-1034 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2020-1038 - Windows Routing Utilities Denial of Service
CVE-2020-1039 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1045 - Microsoft ASP.NET Core Security Feature Bypass Vulnerability
CVE-2020-1052 - Windows Elevation of Privilege Vulnerability
CVE-2020-1053 - DirectX Elevation of Privilege Vulnerability
CVE-2020-1074 - Jet Database Engine Remote Code Execution Vulnerability
CVE-2020-1083 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2020-1091 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2020-1097 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2020-1098 - Windows Shell Infrastructure Component Elevation of Privilege Vulnerability
CVE-2020-1115 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2020-1119 - Windows Information Disclosure Vulnerability
CVE-2020-1122 - Windows Language Pack Installer Elevation of Privilege Vulnerability

CVE-2020-1129 - Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2020-1130 - Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1133 - Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2020-1146 - Microsoft Store Runtime Elevation of Privilege Vulnerability
CVE-2020-1152 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2020-1159 - Windows Elevation of Privilege Vulnerability
CVE-2020-1169 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1228 - Windows DNS Denial of Service Vulnerability
CVE-2020-1245 - Win32k Elevation of Privilege Vulnerability
CVE-2020-1250 - Win32k Information Disclosure Vulnerability
CVE-2020-1252 - Windows Remote Code Execution Vulnerability
CVE-2020-1256 - Windows GDI Information Disclosure Vulnerability
CVE-2020-1285 - GDI+ Remote Code Execution Vulnerability
CVE-2020-1303 - Windows Runtime Elevation of Privilege Vulnerability
CVE-2020-1308 - DirectX Elevation of Privilege Vulnerability
CVE-2020-1319 - Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2020-16851 - OneDrive for Windows Elevation of Privilege Vulnerability
CVE-2020-16852 - OneDrive for Windows Elevation of Privilege Vulnerability
CVE-2020-16853 - OneDrive for Windows Elevation of Privilege Vulnerability
CVE-2020-16854 - Windows Kernel Information Disclosure Vulnerability
CVE-2020-16871 - Microsoft Dynamics 365 (On-Premise) Cross Site Scripting Vulnerability
CVE-2020-16873 - Xamarin.Forms Spoofing Vulnerability
CVE-2020-16874 - Visual Studio Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows Server, version 1903 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
Windows 10 Version 1803 for x64-based Systems
Windows 8.1 for x64-based systems
Microsoft Visual Studio 2012 Update 5
OneDrive for Windows
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Microsoft Dynamics 365 (on-premises) version 8.2
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems

Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 2004 for ARM64-based Systems
Microsoft Visual Studio 2015 Update 3
xamarin.forms
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 1903 for ARM64-based Systems
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows 10 Version 1809 for x64-based Systems
ASP.NET Core 2.1
Dynamics 365 for Finance and Operations
Windows Server 2012
Microsoft Visual Studio 2013 Update 5
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
ASP.NET Core 3.1
Windows Server, version 1909 (Server Core installation)
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Windows 10 Version 1709 for ARM64-based Systems
Windows Server, version 1803 (Server Core Installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0914
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0922
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1159
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1031

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1052
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16861
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1532
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0766
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1033
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0718
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16852
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0837
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0911
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16851
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1250
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16873
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1590
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1376
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1596
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16859
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1508
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1129
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1252
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16862
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16864
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1589
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1592
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1045

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16878
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16871
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16857
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0886
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1030
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0951
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1098
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1122
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0989
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0870
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16853
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0908
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0648
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1169
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0805
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0941
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1507
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1115
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16881
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1245
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1130
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0998
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1146
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1471

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1074
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16874
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0664
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1228
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0838
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1119
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1038
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0875
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0782
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16860
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0997
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1598
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1034
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0761
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1303
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1559
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1091
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1319
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1083
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0921
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16856
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0912
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1013
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1593

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16854
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16858
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1053
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0928
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1039
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1152
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1097
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16872
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1285
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0839
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1491
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0790
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-16879
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1256
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0890
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0856
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1308
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1133
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0904
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-0836
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0890
URL	https://support.microsoft.com/en-us/help/4571756
URL	https://support.microsoft.com/en-us/help/4570333
URL	https://support.microsoft.com/en-us/help/4577041

Type	Reference
URL	https://support.microsoft.com/en-us/help/4577015
URL	https://support.microsoft.com/en-us/help/4577049
URL	https://support.microsoft.com/en-us/help/4577032
URL	https://support.microsoft.com/en-us/help/4574727
URL	https://support.microsoft.com/en-us/help/4577064
URL	https://support.microsoft.com/en-us/help/4577066
URL	https://support.microsoft.com/en-us/help/4577051
URL	https://support.microsoft.com/en-us/help/4577038
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1471
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1074
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16874
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0664
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1228
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0838
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0922
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0914
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1159
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1119
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1038

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1031
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1052
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0875
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16861
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0782
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16860
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1033
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0997
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0766
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1532
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1598
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1034
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0761
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1303
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1559
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1091

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1319
URL	https://support.microsoft.com/en-us/help/4577071
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0718
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16852
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0837
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16851
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0911
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1083
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0921
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1250
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16873
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1590
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16856
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1596
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1376
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0912

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1013
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1508
URL	https://support.microsoft.com/en-us/help/4571481
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16859
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1129
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1252
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1593
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16854
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16858
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0928
URL	https://support.microsoft.com/en-us/help/4577070
URL	https://support.microsoft.com/en-us/help/4571479
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1053
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16862
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16864
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1589
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1592

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1039
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1045
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1152
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1097
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16878
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16871
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16857
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16872
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0886
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1098
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0951
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1030
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1285
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0839
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1122
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1491

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0989
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0870
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16853
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0790
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16879
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0908
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1256
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0648
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1169
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0805
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0941
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1507
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1115
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1245
URL	https://support.microsoft.com/en-us/help/4577053
URL	https://support.microsoft.com/en-us/help/4577048

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-16881
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0856
URL	https://support.microsoft.com/en-us/help/4576950
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1130
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1308
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0998
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1133
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0904
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1146
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0836
URL	https://support.microsoft.com/en-us/help/4571480
URL	https://support.microsoft.com/en-us/help/4574742
URL	https://support.microsoft.com/en-us/help/4577501

MS21-APR: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their April 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-27067 - Azure DevOps Server and Team Foundation Server Information Disclosure

Vulnerability
CVE-2021-27072 - Win32k Elevation of Privilege Vulnerability
CVE-2021-27079 - Windows Media Photo Codec Information Disclosure Vulnerability
CVE-2021-27088 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-27089 - Microsoft Internet Messaging API Remote Code Execution Vulnerability
CVE-2021-27090 - Windows Secure Kernel Mode Elevation of Privilege Vulnerability
CVE-2021-27091 - RPC Endpoint Mapper Service Elevation of Privilege Vulnerability
CVE-2021-27092 - Azure AD Web Sign-in Security Feature Bypass Vulnerability
CVE-2021-27093 - Windows Kernel Information Disclosure Vulnerability
CVE-2021-27094 - Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability
CVE-2021-27095 - Windows Media Video Decoder Remote Code Execution Vulnerability
CVE-2021-27096 - NTFS Elevation of Privilege Vulnerability
CVE-2021-26413 - Windows Installer Spoofing Vulnerability
CVE-2021-26415 - Windows Installer Elevation of Privilege Vulnerability
CVE-2021-26416 - Windows Hyper-V Denial of Service Vulnerability
CVE-2021-26417 - Windows Overlay Filter Information Disclosure Vulnerability
CVE-2021-28309 - Windows Kernel Information Disclosure Vulnerability
CVE-2021-28310 - Win32k Elevation of Privilege Vulnerability
CVE-2021-28311 - Windows Application Compatibility Cache Denial of Service Vulnerability
CVE-2021-28312 - Windows NTFS Denial of Service Vulnerability
CVE-2021-28313 - Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2021-28314 - Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2021-28315 - Windows Media Video Decoder Remote Code Execution Vulnerability
CVE-2021-28316 - Windows WLAN AutoConfig Service Security Feature Bypass Vulnerability
CVE-2021-28317 - Microsoft Windows Codecs Library Information Disclosure Vulnerability
CVE-2021-28318 - Windows GDI+ Information Disclosure Vulnerability
CVE-2021-28319 - Windows TCP/IP Driver Denial of Service Vulnerability
CVE-2021-28320 - Windows Resource Manager PSM Service Extension Elevation of Privilege Vulnerability
CVE-2021-28321 - Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2021-28322 - Diagnostics Hub Standard Collector Service Elevation of Privilege Vulnerability
CVE-2021-28323 - Windows DNS Information Disclosure Vulnerability
CVE-2021-28324 - Windows SMB Information Disclosure Vulnerability
CVE-2021-28325 - Windows SMB Information Disclosure Vulnerability
CVE-2021-28326 - Windows AppX Deployment Server Denial of Service Vulnerability
CVE-2021-28327 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28328 - Windows DNS Information Disclosure Vulnerability
CVE-2021-28329 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28330 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28331 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28332 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28333 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28334 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28335 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28336 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28337 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28338 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28339 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28340 - Remote Procedure Call Runtime Remote Code Execution Vulnerability

CVE-2021-28341 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28342 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28343 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28344 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28345 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28346 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28347 - Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2021-28348 - Windows GDI+ Remote Code Execution Vulnerability
CVE-2021-28349 - Windows GDI+ Remote Code Execution Vulnerability
CVE-2021-28350 - Windows GDI+ Remote Code Execution Vulnerability
CVE-2021-28351 - Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2021-28352 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28353 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28354 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28355 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28356 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28357 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28358 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28434 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-28435 - Windows Event Tracing Information Disclosure Vulnerability
CVE-2021-28436 - Windows Speech Runtime Elevation of Privilege Vulnerability
CVE-2021-28437 - Windows Installer Information Disclosure Vulnerability
CVE-2021-28438 - Windows Console Driver Denial of Service Vulnerability
CVE-2021-28439 - Windows TCP/IP Driver Denial of Service Vulnerability
CVE-2021-28440 - Windows Installer Elevation of Privilege Vulnerability
CVE-2021-28441 - Windows Hyper-V Information Disclosure Vulnerability
CVE-2021-28442 - Windows TCP/IP Information Disclosure Vulnerability
CVE-2021-28443 - Windows Console Driver Denial of Service Vulnerability
CVE-2021-28444 - Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2021-28445 - Windows Network File System Remote Code Execution Vulnerability
CVE-2021-28446 - Windows Portmapping Information Disclosure Vulnerability
CVE-2021-28447 - Windows Early Launch Antimalware Driver Security Feature Bypass Vulnerability
CVE-2021-28448 - Visual Studio Code Kubernetes Tools Remote Code Execution Vulnerability
CVE-2021-28457 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-28458 - Azure ms-rest-nodeauth Library Elevation of Privilege Vulnerability
CVE-2021-28459 - Azure DevOps Server Spoofing Vulnerability
CVE-2021-28460 - Azure Sphere Unsigned Code Execution Vulnerability
CVE-2021-28469 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-28470 - Visual Studio Code GitHub Pull Requests and Issues Extension Remote Code Execution Vulnerability
CVE-2021-28471 - Remote Development Extension for Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-28472 - Visual Studio Code Maven for Java Extension Remote Code Execution Vulnerability
CVE-2021-28475 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-28477 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-27064 - Visual Studio Installer Elevation of Privilege Vulnerability
CVE-2021-27086 - Windows Services and Controller App Elevation of Privilege Vulnerability
CVE-2021-28464 - VP9 Video Extensions Remote Code Execution Vulnerability
CVE-2021-28466 - Raw Image Extension Remote Code Execution Vulnerability

CVE-2021-28468 - Raw Image Extension Remote Code Execution Vulnerability
CVE-2021-28473 - Visual Studio Code Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows 10 Version 1803 for x64-based Systems
Raw Image Extension
Windows 8.1 for x64-based systems
Windows 10 Version 20H2 for ARM64-based Systems
Azure DevOps Server 2020.0.1
@azure/ms-rest-nodeauth
Windows 10 Version 1909 for x64-based Systems
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Azure DevOps Server 2019 Update 1
Windows 10 Version 1803 for 32-bit Systems
Team Foundation Server 2018 Update 3.2
Visual Studio Code - Kubernetes Tools
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Azure DevOps Server 2019.0.1
Windows 10 Version 2004 for ARM64-based Systems
Microsoft Visual Studio 2015 Update 3
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
VP9 Video Extensions
Windows Server, version 2004 (Server Core installation)
Azure Sphere
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows 10 Version 1809 for x64-based Systems
Azure DevOps Server 2020
Windows Server, version 20H2 (Server Core Installation)
Visual Studio Code - GitHub Pull Requests and Issues Extension
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)

Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows Server, version 1909 (Server Core installation)
Visual Studio Code - Maven for Java Extension
Team Foundation Server 2017 Update 3.1
Windows 10 Version 1909 for ARM64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Team Foundation Server 2018 Update 1.2
Windows Server 2019 (Server Core installation)
Windows Server 2016
Team Foundation Server 2015 Update 4.2
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Azure DevOps Server 2019 Update 1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28464
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28442
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28457
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27088
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28443
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28329
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28343
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28438
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28331
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26413
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28353

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28352
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28313
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28348
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27095
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27067
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27079
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28338
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28446
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28475
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28458
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27093
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28327
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28437
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27096
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27091
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28466
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28323
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28319
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28477
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26417
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28312
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28315
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28355
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28459

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28351
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28472
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28345
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27094
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26416
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28344
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28309
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28318
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28328
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28324
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28447
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28473
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27090
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28340
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28439
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27064
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28326
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28448
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28332
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28435
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28333
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27072
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28317
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28310

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28316
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28322
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28346
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28354
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28325
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28356
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28468
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28330
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28341
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28436
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28342
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28460
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28335
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27092
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28440
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28334
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28320
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28441
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28434
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28321
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28337
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28339
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28444
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28336

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28471
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28357
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28350
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27089
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28470
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27086
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28311
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28314
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28347
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28445
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28469
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26415
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28358
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28349
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28351
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28355
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28315
URL	https://support.microsoft.com/en-us/help/5001389
URL	https://support.microsoft.com/en-us/help/5001387
URL	https://support.microsoft.com/en-us/help/5001330
URL	https://support.microsoft.com/en-us/help/5001342
URL	https://support.microsoft.com/en-us/help/5001340
URL	https://support.microsoft.com/en-us/help/5001339

Type	Reference
URL	https://support.microsoft.com/en-us/help/5001292
URL	https://support.microsoft.com/en-us/help/5001347
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27086
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28314
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28311
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28347
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28469
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28445
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26415
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28327
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27093
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28437
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27096
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28466
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27091
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28323

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28477
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28319
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26417
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28312
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28352
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28313
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28348
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27095
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27067
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28317
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27072
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28333
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28332
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28435
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28326
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28448

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27064
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28340
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28439
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27090
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28447
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28473
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28324
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28318
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28328
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28309
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28344
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26416
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27094
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28345
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28472
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28459

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27089
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28470
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28357
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28350
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28471
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28336
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28444
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28339
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28337
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28321
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28434
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28441
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28334
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28320
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28440
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28358

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28349
URL	https://support.microsoft.com/en-us/help/5001383
URL	https://support.microsoft.com/en-us/help/5001335
URL	https://support.microsoft.com/en-us/help/5001382
URL	https://support.microsoft.com/en-us/help/5001332
URL	https://support.microsoft.com/en-us/help/5001337
URL	https://support.microsoft.com/en-us/help/5001393
URL	https://support.microsoft.com/en-us/help/5001392
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27092
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28335
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28460
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28342
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28436
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28341
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28330
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28468
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28356
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28325

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28354
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28346
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28322
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28316
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28310
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28343
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28438
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28331
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28464
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28457
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28442
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27088
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28443
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28329
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27079
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28475

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28446
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26413
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28353
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28338
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28458

MS21-AUG: Microsoft Internet Explorer Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2021-34480 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows 10 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows Server 2016
Windows 8.1 for 32-bit systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 21H1 for ARM64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their August 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34480
URL	https://support.microsoft.com/en-us/help/5005043
URL	https://support.microsoft.com/en-us/help/5005030
URL	https://support.microsoft.com/en-us/help/5005033
URL	https://support.microsoft.com/en-us/help/5005040
URL	https://support.microsoft.com/en-us/help/5005076
URL	https://support.microsoft.com/en-us/help/5005031
URL	https://support.microsoft.com/en-us/help/5005099
URL	https://support.microsoft.com/en-us/help/5005036
URL	https://support.microsoft.com/en-us/help/5005088

MS21-AUG: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-33762 - Azure CycleCloud Elevation of Privilege Vulnerability
CVE-2021-34524 - Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability
CVE-2021-34480 - Scripting Engine Memory Corruption Vulnerability
CVE-2021-34486 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-34536 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-34487 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-34537 - Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2021-26423 - .NET Core and Visual Studio Denial of Service Vulnerability
CVE-2021-26424 - Windows TCP/IP Remote Code Execution Vulnerability
CVE-2021-26425 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-26426 - Windows User Account Profile Picture Elevation of Privilege Vulnerability
CVE-2021-26428 - Azure Sphere Information Disclosure Vulnerability
CVE-2021-26429 - Azure Sphere Elevation of Privilege Vulnerability
CVE-2021-26430 - Azure Sphere Denial of Service Vulnerability
CVE-2021-36936 - Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-36937 - Windows Media MPEG-4 Video Decoder Remote Code Execution Vulnerability
CVE-2021-36938 - Windows Cryptographic Primitives Library Information Disclosure Vulnerability
CVE-2021-36942 - Windows LSA Spoofing Vulnerability
CVE-2021-36945 - Windows 10 Update Assistant Elevation of Privilege Vulnerability
CVE-2021-36946 - Microsoft Dynamics Business Central Cross-site Scripting Vulnerability
CVE-2021-36947 - Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-36948 - Windows Update Medic Service Elevation of Privilege Vulnerability
CVE-2021-36949 - Microsoft Azure Active Directory Connect Authentication Bypass Vulnerability
CVE-2021-36950 - Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability
CVE-2021-34471 - Microsoft Windows Defender Elevation of Privilege Vulnerability
CVE-2021-34530 - Windows Graphics Component Remote Code Execution Vulnerability
CVE-2021-34532 - ASP.NET Core and Visual Studio Information Disclosure Vulnerability
CVE-2021-34533 - Windows Graphics Component Font Parsing Remote Code Execution Vulnerability
CVE-2021-34483 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-34484 - Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2021-34485 - .NET Core and Visual Studio Information Disclosure Vulnerability
CVE-2021-34535 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2021-26431 - Windows Recovery Environment Agent Elevation of Privilege Vulnerability
CVE-2021-26432 - Windows Services for NFS ONCRPC XDR Driver Remote Code Execution Vulnerability
CVE-2021-26433 - Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-36926 - Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-36927 - Windows Digital TV Tuner device registration application Elevation of Privilege Vulnerability
CVE-2021-36932 - Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-36933 - Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2021-36943 - Azure CycleCloud Elevation of Privilege Vulnerability
CVE-2021-30590 - Chromium: CVE-2021-30590 Heap buffer overflow in Bookmarks
CVE-2021-30591 - Chromium: CVE-2021-30591 Use after free in File System API
CVE-2021-30592 - Chromium: CVE-2021-30592 Out of bounds write in Tab Groups
CVE-2021-30593 - Chromium: CVE-2021-30593 Out of bounds read in Tab Strip
CVE-2021-30594 - Chromium: CVE-2021-30594 Use after free in Page Info UI
CVE-2021-30596 - Chromium: CVE-2021-30596 Incorrect security UI in Navigation
CVE-2021-30597 - Chromium: CVE-2021-30597 Use after free in Browser UI

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Microsoft Azure Active Directory Connect 2.0.3.0
Windows Server 2012 (Server Core installation)
Dynamics 365 Business Central 2019 Spring Update
Windows Server 2019
.NET 5.0
Windows 8.1 for x64-based systems
Visual Studio 2019 for Mac version 8.10
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Remote Desktop client for Windows Desktop
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Dynamics 365 (on-premises) version 9.1
Windows 10 Version 2004 for ARM64-based Systems
Azure CycleCloud 7.9.10
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows Server, version 2004 (Server Core installation)
Azure Sphere
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H1 for ARM64-based Systems
ASP.NET Core 2.1
Windows Server, version 20H2 (Server Core Installation)
Microsoft Malware Protection Engine
Microsoft Edge (Chromium-based)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Azure CycleCloud 8.2.0
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Dynamics 365 Business Central 2020 Release Wave 2 - Update 17.9
Windows Server 2012 R2 (Server Core installation)
Windows Update Assistant
Windows Server 2012 R2

Windows 8.1 for 32-bit systems
ASP.NET Core 3.1
Microsoft Azure Active Directory Connect 1.6.4.0
Microsoft Visual Studio 2019 version 16.10 (includes 16.0 - 16.9)
.NET Core 3.1
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
.NET Core 2.1
Microsoft Dynamics NAV 2018
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Microsoft Dynamics NAV 2017
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server 2019 (Server Core installation)
ASP.NET Core 5.0
Windows Server 2016
Microsoft Dynamics 365 Business Central 2020 Release Wave 1 - Update 16.15
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Solution Details

Microsoft has released a fix for this flaw in their August 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34486
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34471
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34533
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26424
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34535
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36927
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34532
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36942

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34485
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36936
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26431
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34480
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36950
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26426
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26430
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36938
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34487
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36926
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36949
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36946
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36943
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36937
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34536
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36933
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26423
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33762
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34483
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26428
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34524
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26432
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36945
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26425

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36947
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34537
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26433
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26429
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36932
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34484
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34530
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36948
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30596
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30592
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30590
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30593
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30594
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30591
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30597
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34481
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34537
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26433
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26429
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36932
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34484

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36948
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34530
URL	https://support.microsoft.com/en-us/help/5005033
URL	https://support.microsoft.com/en-us/help/5005369
URL	https://support.microsoft.com/en-us/help/4618795
URL	https://support.microsoft.com/en-us/help/5005370
URL	https://support.microsoft.com/en-us/help/4023814
URL	https://support.microsoft.com/en-us/help/5005095
URL	https://support.microsoft.com/en-us/help/5005090
URL	https://support.microsoft.com/en-us/help/5005040
URL	https://support.microsoft.com/en-us/help/5005374
URL	https://support.microsoft.com/en-us/help/5005373
URL	https://support.microsoft.com/en-us/help/5005076
URL	https://support.microsoft.com/en-us/help/5005031
URL	https://support.microsoft.com/en-us/help/5005106
URL	https://support.microsoft.com/en-us/help/5005089
URL	https://support.microsoft.com/en-us/help/5005099
URL	https://support.microsoft.com/en-us/help/5005036
URL	https://support.microsoft.com/en-us/help/5005088
URL	https://support.microsoft.com/en-us/help/5005094
URL	https://support.microsoft.com/en-us/help/5005239
URL	https://support.microsoft.com/en-us/help/5005368
URL	https://support.microsoft.com/en-us/help/4618809

Type	Reference
URL	https://support.microsoft.com/en-us/help/5005043
URL	https://support.microsoft.com/en-us/help/5005030
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34486
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34471
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34534
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34533
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26424
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34535
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36927
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34532
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36942
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34485
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30594
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36936
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26431
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34480

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36950
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26426
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26430
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30592
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36938
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30590
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34487
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36926
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30591
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36949
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36943
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36946
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36937
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30593
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34536
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36933

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26423
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30596
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33762
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34483
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26428
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34524
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26432
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36945
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26425
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36947
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30597
URL	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-34481

MS21-DEC: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their December 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-40441 - Windows Media Center Elevation of Privilege Vulnerability

CVE-2021-40452 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-40453 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-42310 - Microsoft Defender for IoT Remote Code Execution Vulnerability
CVE-2021-42311 - Microsoft Defender for IoT Remote Code Execution Vulnerability
CVE-2021-42312 - Microsoft Defender for IOT Elevation of Privilege Vulnerability
CVE-2021-42313 - Microsoft Defender for IoT Remote Code Execution Vulnerability
CVE-2021-42314 - Microsoft Defender for IoT Remote Code Execution Vulnerability
CVE-2021-42315 - Microsoft Defender for IoT Remote Code Execution Vulnerability
CVE-2021-43214 - Web Media Extensions Remote Code Execution Vulnerability
CVE-2021-43215 - iSNS Server Memory Corruption Vulnerability Can Lead to Remote Code Execution
CVE-2021-43216 - Microsoft Local Security Authority Server (lsasrv) Information Disclosure Vulnerability
CVE-2021-43217 - Windows Encrypting File System (EFS) Remote Code Execution Vulnerability
CVE-2021-43219 - DirectX Graphics Kernel File Denial of Service Vulnerability
CVE-2021-43222 - Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2021-43223 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2021-43224 - Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2021-43225 - Bot Framework SDK Remote Code Execution Vulnerability
CVE-2021-43226 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-43227 - Storage Spaces Controller Information Disclosure Vulnerability
CVE-2021-43228 - SymCrypt Denial of Service Vulnerability
CVE-2021-43229 - Windows NTFS Elevation of Privilege Vulnerability
CVE-2021-43230 - Windows NTFS Elevation of Privilege Vulnerability
CVE-2021-43231 - Windows NTFS Elevation of Privilege Vulnerability
CVE-2021-43232 - Windows Event Tracing Remote Code Execution Vulnerability
CVE-2021-43233 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2021-43234 - Windows Fax Service Remote Code Execution Vulnerability
CVE-2021-43235 - Storage Spaces Controller Information Disclosure Vulnerability
CVE-2021-43236 - Microsoft Message Queuing Information Disclosure Vulnerability
CVE-2021-43237 - Windows Setup Elevation of Privilege Vulnerability
CVE-2021-43238 - Windows Remote Access Elevation of Privilege Vulnerability
CVE-2021-43239 - Windows Recovery Environment Agent Elevation of Privilege Vulnerability
CVE-2021-43240 - NTFS Set Short Name Elevation of Privilege Vulnerability
CVE-2021-43243 - VP9 Video Extensions Information Disclosure Vulnerability
CVE-2021-43244 - Windows Kernel Information Disclosure Vulnerability
CVE-2021-43245 - Windows Digital TV Tuner Elevation of Privilege Vulnerability
CVE-2021-43246 - Windows Hyper-V Denial of Service Vulnerability
CVE-2021-43247 - Windows TCP/IP Driver Elevation of Privilege Vulnerability
CVE-2021-43248 - Windows Digital Media Receiver Elevation of Privilege Vulnerability
CVE-2021-43877 - ASP.NET Core and Visual Studio Elevation of Privilege Vulnerability
CVE-2021-43882 - Microsoft Defender for IoT Remote Code Execution Vulnerability
CVE-2021-43888 - Microsoft Defender for IoT Information Disclosure Vulnerability
CVE-2021-43889 - Microsoft Defender for IoT Remote Code Execution Vulnerability
CVE-2021-43891 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-43899 - Microsoft 4K Wireless Display Adapter Remote Code Execution Vulnerability
CVE-2021-43907 - Visual Studio Code WSL Extension Remote Code Execution Vulnerability
CVE-2021-41333 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-41360 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-41365 - Microsoft Defender for IoT Remote Code Execution Vulnerability
CVE-2021-43207 - Windows Common Log File System Driver Elevation of Privilege Vulnerability

CVE-2021-43880 - Windows Mobile Device Management Elevation of Privilege Vulnerability
CVE-2021-43883 - Windows Installer Elevation of Privilege Vulnerability
CVE-2021-43890 - Windows AppX Installer Spoofing Vulnerability
CVE-2021-43892 - Microsoft BizTalk ESB Toolkit Spoofing Vulnerability
CVE-2021-43893 - Windows Encrypting File System (EFS) Elevation of Privilege Vulnerability
CVE-2021-43896 - Microsoft PowerShell Spoofing Vulnerability
CVE-2021-43908 - Visual Studio Code Spoofing Vulnerability
CVE-2021-4052 - Chromium: CVE-2021-4052 Use after free in web apps
CVE-2021-4053 - Chromium: CVE-2021-4053 Use after free in UI
CVE-2021-4054 - Chromium: CVE-2021-4054 Incorrect security UI in autofill
CVE-2021-4055 - Chromium: CVE-2021-4055 Heap buffer overflow in extensions
CVE-2021-4056 - Chromium: CVE-2021-4056: Type Confusion in loader
CVE-2021-4057 - Chromium: CVE-2021-4057 Use after free in file API
CVE-2021-4058 - Chromium: CVE-2021-4058 Heap buffer overflow in ANGLE
CVE-2021-4059 - Chromium: CVE-2021-4059 Insufficient data validation in loader
CVE-2021-4061 - Chromium: CVE-2021-4061 Type Confusion in V8
CVE-2021-4062 - Chromium: CVE-2021-4062 Heap buffer overflow in BFCache
CVE-2021-4063 - Chromium: CVE-2021-4063 Use after free in developer tools
CVE-2021-4064 - Chromium: CVE-2021-4064 Use after free in screen capture
CVE-2021-4065 - Chromium: CVE-2021-4065 Use after free in autofill
CVE-2021-4066 - Chromium: CVE-2021-4066 Integer underflow in ANGLE
CVE-2021-4067 - Chromium: CVE-2021-4067 Use after free in window manager
CVE-2021-4068 - Chromium: CVE-2021-4068 Insufficient validation of untrusted input in new tab page
CVE-2021-4098 - Chromium: CVE-2021-4098 Insufficient data validation in Mojo
CVE-2021-4099 - Chromium: CVE-2021-4099 Use after free in Swiftshader
CVE-2021-4100 - Chromium: CVE-2021-4100 Object lifecycle issue in ANGLE
CVE-2021-4101 - Chromium: CVE-2021-4101 Heap buffer overflow in Swiftshader
CVE-2021-4102 - Chromium: CVE-2021-4102 Use after free in V8

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
HEVC Video Extensions
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
ASP.NET Core 6.0
Windows Server 2012 (Server Core installation)
Windows Server 2022 (Server Core installation)
Windows Server 2019
Visual Studio Code WSL Extension
Microsoft BizTalk ESB Toolkit 2.2
Raw Image Extension
Windows 8.1 for x64-based systems
Bot Framework SDK for .NET Framework
Windows 10 Version 21H2 for ARM64-based Systems

Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 11 for x64-based Systems
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
App Installer
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Defender for IoT
VP9 Video Extensions
Windows Server, version 2004 (Server Core installation)
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows 10 Version 1809 for x64-based Systems
Microsoft BizTalk ESB Toolkit 2.4
Windows 10 Version 21H1 for ARM64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Microsoft Edge (Chromium-based)
Windows 10 Version 21H2 for x64-based Systems
Windows Server 2022
Microsoft Visual Studio 2022 version 17.0
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
PowerShell 7.2
Windows 8.1 for 32-bit systems
ASP.NET Core 3.1
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 11 for ARM64-based Systems
Microsoft BizTalk ESB Toolkit 2.3
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
ASP.NET Core 5.0
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft 4K Wireless Display Adapter

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43893
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43215
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43217
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43246
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43235
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43230
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43877
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42314
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43214
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43223
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41365
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41333
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43883
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42315
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43889
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43233
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43228
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43907
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43899
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40441

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43896
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43219
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43232
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40452
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43248
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43908
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43247
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43238
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43239
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42310
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43236
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43243
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43207
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40453
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43237
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43224
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43880
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42313
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43240
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43227
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43891
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43231
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43244
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43245

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42312
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43225
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43222
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42311
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43229
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43234
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43226
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43888
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41360
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43216
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43892
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43890
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43882
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4055
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4062
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4052
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4061
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4057
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4063
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4067
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4064
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4053
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4066
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4054

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4068
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4058
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4065
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4059
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4056
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4098
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4101
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4099
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4100
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-4102
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43207
URL	https://support.microsoft.com/en-us/help/5008206
URL	https://support.microsoft.com/en-us/help/5008271
URL	https://support.microsoft.com/en-us/help/5008223
URL	https://support.microsoft.com/en-us/help/5008255
URL	https://support.microsoft.com/en-us/help/5008285
URL	https://support.microsoft.com/en-us/help/5009301
URL	https://support.microsoft.com/en-us/help/5008263
URL	https://support.microsoft.com/en-us/help/5008210
URL	https://support.microsoft.com/en-us/help/5008282
URL	https://support.microsoft.com/en-us/help/5008274
URL	https://support.microsoft.com/en-us/help/5008230
URL	https://support.microsoft.com/en-us/help/5008218
URL	https://support.microsoft.com/en-us/help/5008212

Type	Reference
URL	https://support.microsoft.com/en-us/help/5008277
URL	https://support.microsoft.com/en-us/help/5008207
URL	https://support.microsoft.com/en-us/help/5008215
URL	https://support.microsoft.com/en-us/help/5008244
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43893
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43215
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4098
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43217
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4101
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4063
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43246
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43235
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43230
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43877
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42314
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43214
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43223

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41365
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41333
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43883
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42315
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43889
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43233
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4100
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43228
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4065
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43907
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4056
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4102
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4055
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43899
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40441
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4057

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4067
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4064
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4053
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43896
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43219
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4054
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43232
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40452
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43248
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4068
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4058
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43908
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43247
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43238
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4062
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43239

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42310
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43236
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43243
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40453
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43237
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43224
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43880
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4099
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42313
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43240
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43227
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43891
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4059
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43231
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43244
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43245

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42312
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4052
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43225
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4061
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43222
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42311
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43229
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-4066
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43234
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43226
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43888
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41360
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43216
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43892
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43882
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43890

MS21-FEB: Microsoft Windows Security Update

High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their February 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-1639 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-1721 - .NET Core and Visual Studio Denial of Service Vulnerability
CVE-2021-1724 - Microsoft Dynamics Business Central Cross-site Scripting Vulnerability
CVE-2021-1728 - System Center Operations Manager Elevation of Privilege Vulnerability
CVE-2021-1731 - PFX Encryption Security Feature Bypass Vulnerability
CVE-2021-1732 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-1733 - Sysinternals PsExec Elevation of Privilege Vulnerability
CVE-2021-1734 - Windows Remote Procedure Call Information Disclosure Vulnerability
CVE-2021-1698 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-1722 - Windows Fax Service Remote Code Execution Vulnerability
CVE-2021-25195 - Windows PKU2U Elevation of Privilege Vulnerability
CVE-2021-24087 - Azure IoT CLI extension Elevation of Privilege Vulnerability
CVE-2021-24093 - Windows Graphics Component Remote Code Execution Vulnerability
CVE-2021-24096 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-24101 - Microsoft Dataverse Information Disclosure Vulnerability
CVE-2021-24112 - .NET Core Remote Code Execution Vulnerability
CVE-2021-26700 - Visual Studio Code npm-script Extension Remote Code Execution Vulnerability
CVE-2021-26701 - .NET Core Remote Code Execution Vulnerability
CVE-2021-24114 - Microsoft Teams iOS Information Disclosure Vulnerability
CVE-2021-1727 - Windows Installer Elevation of Privilege Vulnerability
CVE-2021-24074 - Windows TCP/IP Remote Code Execution Vulnerability
CVE-2021-24075 - Windows Network File System Denial of Service Vulnerability
CVE-2021-24076 - Microsoft Windows VMSwitch Information Disclosure Vulnerability
CVE-2021-24077 - Windows Fax Service Remote Code Execution Vulnerability
CVE-2021-24078 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-24079 - Windows Backup Engine Information Disclosure Vulnerability
CVE-2021-24080 - Windows Trust Verification API Denial of Service Vulnerability
CVE-2021-24081 - Microsoft Windows Codecs Library Remote Code Execution Vulnerability
CVE-2021-24082 - Microsoft.PowerShell.Utility Module WDAC Security Feature Bypass Vulnerability
CVE-2021-24083 - Windows Address Book Remote Code Execution Vulnerability
CVE-2021-24084 - Windows Mobile Device Management Information Disclosure Vulnerability
CVE-2021-24086 - Windows TCP/IP Denial of Service Vulnerability
CVE-2021-24088 - Windows Local Spooler Remote Code Execution Vulnerability

CVE-2021-24091 - Windows Camera Codec Pack Remote Code Execution Vulnerability
CVE-2021-24092 - Microsoft Defender Elevation of Privilege Vulnerability
CVE-2021-24094 - Windows TCP/IP Remote Code Execution Vulnerability
CVE-2021-24098 - Windows Console Driver Denial of Service Vulnerability
CVE-2021-24102 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-24103 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-24105 - Package Managers Configurations Remote Code Execution Vulnerability
CVE-2021-24106 - Windows DirectX Information Disclosure Vulnerability
CVE-2021-24109 - Microsoft Azure Kubernetes Service Elevation of Privilege Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows Defender on Windows Server 2019
Windows Defender on Windows Server 2012
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Microsoft Dynamics 365 Business Central 2020 Release Wave 1
Windows 10 Version 20H2 for 32-bit Systems
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Defender on Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019
Windows Defender on Windows Server 2016 (Server Core installation)
Microsoft System Center 2012 R2 Endpoint Protection
Windows Defender on Windows Server 2012 R2 (Server Core installation)
Windows Defender on Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows Defender on Windows 10 Version 1903 for x64-based Systems
azure-iot-cli-extension
.NET 5.0
Windows Defender on Windows Server 2016
Windows 8.1 for x64-based systems
Windows Defender on Windows 7 for 32-bit Systems Service Pack 1
Windows Defender on Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows Defender on Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Microsoft Dynamics 365 (on-premises) version 8.2
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Azure Kubernetes Service

Visual Studio Code - npm-script Extension
Windows 10 Version 2004 for ARM64-based Systems
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Security Essentials
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server, version 2004 (Server Core installation)
Windows Defender on Windows 10 for 32-bit Systems
Microsoft Endpoint Protection
Windows Defender on Windows 10 Version 1803 for x64-based Systems
Windows Defender on Windows 10 for x64-based Systems
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows 10 Version 1809 for x64-based Systems
Package Manager Configurations
Windows Defender on Windows 10 Version 20H2 for 32-bit Systems
Windows Defender on Windows 10 Version 20H2 for ARM64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Microsoft System Center 2012 Endpoint Protection
System Center 2019 Operations Manager
Windows Defender on Windows Server, version 20H2 (Server Core Installation)
Windows Defender on Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1903 for ARM64-based Systems
Dynamics 365 Business Central 2019 Release Wave 2 (On-Premise)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Defender on Windows 10 Version 1803 for 32-bit Systems
Visual Studio Code
Windows Defender on Windows 10 Version 1903 for 32-bit Systems
Microsoft Teams for iOS
Windows Defender on Windows Server, version 2004 (Server Core installation)
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft Dynamics NAV 2015
Windows Defender on Windows 10 Version 1607 for 32-bit Systems
Windows Defender on Windows 10 Version 1909 for ARM64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Defender on Windows 10 Version 2004 for x64-based Systems
Windows 8.1 for 32-bit systems
Windows Defender on Windows 10 Version 1607 for x64-based Systems
Windows Defender on Windows 8.1 for x64-based systems
Windows Defender on Windows Server 2019 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
.NET Core 3.1
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
PsExec
Windows Defender on Windows Server, version 1909 (Server Core installation)
Windows 10 Version 1909 for ARM64-based Systems

Windows Defender on Windows 10 Version 2004 for ARM64-based Systems
Windows Defender on Windows Server, version 1903 (Server Core installation)
.NET Core 2.1
Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Dynamics NAV 2016
Microsoft Dynamics NAV 2018
Windows Defender on Windows 10 Version 1809 for 32-bit Systems
Microsoft Dynamics NAV 2017
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows Defender on Windows 10 Version 1909 for x64-based Systems
Windows Defender on Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Defender on Windows Server 2012 R2
Windows 10 Version 1803 for ARM64-based Systems
Windows Defender on Windows 10 Version 1809 for ARM64-based Systems
Microsoft System Center Endpoint Protection
Microsoft Visual Studio 2019 version 16.8
Windows Defender on Windows Server 2012 (Server Core installation)
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows 7 for x64-based Systems Service Pack 1
Microsoft Dynamics 365 Business Central 2020 Release Wave 2

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-25195
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26700
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24091
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24078
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26701
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24082
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24096
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1731
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24087

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1728
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24105
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24081
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1698
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24077
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1639
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24102
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1724
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24084
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24079
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24112
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24101
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24109
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1732
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1722
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24088
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24076
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1734
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24083
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1727
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24075
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1721
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24074
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24094

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24086
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24093
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24098
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24092
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24106
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24103
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24114
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1733
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24080
URL	https://support.microsoft.com/en-us/help/4601357
URL	https://support.microsoft.com/en-us/help/4601349
URL	https://support.microsoft.com/en-us/help/4601315
URL	https://support.microsoft.com/en-us/help/4595463
URL	https://support.microsoft.com/en-us/help/4601347
URL	https://support.microsoft.com/en-us/help/4601348
URL	https://support.microsoft.com/en-us/help/4601354
URL	https://support.microsoft.com/en-us/help/4601360
URL	https://support.microsoft.com/en-us/help/4601384
URL	https://support.microsoft.com/en-us/help/4601331
URL	https://support.microsoft.com/en-us/help/4601366
URL	https://support.microsoft.com/en-us/help/4601269
URL	https://support.microsoft.com/en-us/help/4601363
URL	https://support.microsoft.com/en-us/help/4602915
URL	https://support.microsoft.com/en-us/help/4595460

Type	Reference
URL	https://support.microsoft.com/en-us/help/4601318
URL	https://support.microsoft.com/en-us/help/4601345
URL	https://support.microsoft.com/en-us/help/4601319
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26700
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24078
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24091
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24082
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26701
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1731
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24096
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24087
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1728
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24105
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24081
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1698
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24077
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1639

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24102
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1724
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24084
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24079
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24112
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24101
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24109
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1732
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1722
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24088
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24076
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1734
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24083
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1727
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24075
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1721

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24074
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24094
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-25195
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24086
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24093
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24092
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24098
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24114
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24103
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24106
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1733
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24080

MS21-JAN: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their January 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-1644 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-1643 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-1642 - Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
CVE-2021-1637 - Windows DNS Query Information Disclosure Vulnerability
CVE-2021-1647 - Microsoft Defender Remote Code Execution Vulnerability
CVE-2021-1651 - Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2021-1652 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2021-1653 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2021-1654 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2021-1655 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2021-1656 - TPM Device Driver Information Disclosure Vulnerability
CVE-2021-1657 - Windows Fax Compose Form Remote Code Execution Vulnerability
CVE-2021-1658 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1659 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2021-1660 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1661 - Windows Installer Elevation of Privilege Vulnerability
CVE-2021-1662 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-1663 - Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
CVE-2021-1664 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1665 - GDI+ Remote Code Execution Vulnerability
CVE-2021-1666 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1667 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1668 - Microsoft DTV-DVD Video Decoder Remote Code Execution Vulnerability
CVE-2021-1669 - Windows Remote Desktop Security Feature Bypass Vulnerability
CVE-2021-1670 - Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
CVE-2021-1671 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1672 - Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
CVE-2021-1673 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1674 - Windows Remote Desktop Protocol Core Security Feature Bypass Vulnerability
CVE-2021-1676 - Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability
CVE-2021-1679 - Windows CryptoAPI Denial of Service Vulnerability
CVE-2021-1680 - Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2021-1681 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-1682 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-1683 - Windows Bluetooth Security Feature Bypass Vulnerability
CVE-2021-1684 - Windows Bluetooth Security Feature Bypass Vulnerability
CVE-2021-1685 - Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
CVE-2021-1686 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-1687 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-1688 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2021-1689 - Windows Multipoint Management Elevation of Privilege Vulnerability
CVE-2021-1690 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-1691 - Hyper-V Denial of Service Vulnerability
CVE-2021-1692 - Hyper-V Denial of Service Vulnerability

CVE-2021-1693 - Windows CSC Service Elevation of Privilege Vulnerability
CVE-2021-1694 - Windows Update Stack Elevation of Privilege Vulnerability
CVE-2021-1695 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-1696 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2021-1697 - Windows InstallService Elevation of Privilege Vulnerability
CVE-2021-1708 - Windows GDI+ Information Disclosure Vulnerability
CVE-2021-1709 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-1710 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2020-26870 - Visual Studio Remote Code Execution Vulnerability
CVE-2021-1723 - ASP.NET Core and Visual Studio Denial of Service Vulnerability
CVE-2021-1725 - Bot Framework SDK Information Disclosure Vulnerability
CVE-2021-1650 - Windows Runtime C++ Template Library Elevation of Privilege Vulnerability
CVE-2021-1649 - Active Template Library Elevation of Privilege Vulnerability
CVE-2021-1648 - Microsoft splwow64 Elevation of Privilege Vulnerability
CVE-2021-1646 - Windows WLAN Service Elevation of Privilege Vulnerability
CVE-2021-1645 - Windows Docker Information Disclosure Vulnerability
CVE-2021-1638 - Windows Bluetooth Security Feature Bypass Vulnerability
CVE-2021-1677 - Azure Active Directory Pod Identity Spoofing Vulnerability
CVE-2021-1678 - NTLM Security Feature Bypass Vulnerability
CVE-2021-1699 - Windows (modem.sys) Information Disclosure Vulnerability
CVE-2021-1700 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1701 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2021-1702 - Windows Remote Procedure Call Runtime Elevation of Privilege Vulnerability
CVE-2021-1703 - Windows Event Logging Service Elevation of Privilege Vulnerability
CVE-2021-1704 - Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2021-1706 - Windows LUAFV Elevation of Privilege Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows Defender on Windows Server 2019
Windows Defender on Windows Server 2012
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
HEVC Video Extensions
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 (Server Core installation)
Windows Defender on Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019
Microsoft Visual Studio 2019 version 16.0
Windows Defender on Windows Server 2016 (Server Core installation)
Microsoft System Center 2012 R2 Endpoint Protection
Windows Defender on Windows Server 2012 R2 (Server Core installation)
Windows Defender on Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1803 for x64-based Systems

Windows Defender on Windows Server 2016
Windows 8.1 for x64-based systems
Bot Framework SDK for .NET Framework
Windows Defender on Windows 7 for 32-bit Systems Service Pack 1
Windows Defender on Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows Defender on Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Microsoft Remote Desktop for Android
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Remote Desktop client for Windows Desktop
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Defender on Windows RT 8.1
Microsoft Azure Kubernetes Service
Windows 10 Version 2004 for ARM64-based Systems
Microsoft Visual Studio 2015 Update 3
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Security Essentials
Windows 10 for x64-based Systems
Microsoft Remote Desktop
Windows Server, version 2004 (Server Core installation)
Windows Defender on Windows 10 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows Defender on Windows 10 Version 1803 for x64-based Systems
Windows Defender on Windows 10 for x64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows Defender on Windows 10 Version 20H2 for 32-bit Systems
Windows Defender on Windows 10 Version 20H2 for ARM64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Microsoft System Center 2012 Endpoint Protection
Windows Defender on Windows Server, version 20H2 (Server Core Installation)
Windows Defender on Windows 8.1 for 32-bit systems
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Defender on Windows 10 Version 1803 for 32-bit Systems
Windows Defender on Windows Server, version 2004 (Server Core installation)
Windows Defender on Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Defender on Windows 10 Version 1607 for 32-bit Systems
Windows Defender on Windows 10 Version 1909 for ARM64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Bot Framework SDK for JavaScript
Windows Defender on Windows 10 Version 2004 for x64-based Systems

Windows 8.1 for 32-bit systems
ASP.NET Core 3.1
Windows Defender on Windows 10 Version 1607 for x64-based Systems
Windows Defender on Windows 8.1 for x64-based systems
Windows Defender on Windows Server 2019 (Server Core installation)
Windows Server, version 1909 (Server Core installation)
Windows Defender on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Bot Framework SDK for Python
Windows Defender on Windows Server, version 1909 (Server Core installation)
Windows 10 Version 1909 for ARM64-based Systems
Windows Defender on Windows 10 Version 2004 for ARM64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows Defender on Windows 10 Version 1809 for 32-bit Systems
Windows RT 8.1
Windows Defender on Windows 10 Version 1909 for x64-based Systems
Windows Defender on Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Defender on Windows Server 2012 R2
Windows 10 Version 1803 for ARM64-based Systems
Windows Defender on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Visual Studio 2019 version 16.8
Microsoft System Center Endpoint Protection
Windows Defender on Windows Server 2012 (Server Core installation)
ASP.NET Core 5.0
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Defender on Windows 7 for x64-based Systems Service Pack 1

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1661
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1700
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1695
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1658
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1678
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1690

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1650
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1659
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1662
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1648
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1638
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1706
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1687
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1651
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1696
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1673
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1664
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1679
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1672
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1703
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1677
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1668
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1676
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1671
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1655
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1689
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1647
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1646
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1666
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1656

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1692
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1680
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1665
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1654
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1723
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1704
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1725
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1644
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1681
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1660
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1652
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1709
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1694
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1642
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1708
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1674
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1637
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1683
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1702
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1685
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1667
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1693
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1691
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1684

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1670
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1645
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1657
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1688
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1653
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1682
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1701
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1699
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1697
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1669
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1710
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1663
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1686
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-26870
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1643
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1649
URL	https://support.microsoft.com/en-us/help/4598230
URL	https://support.microsoft.com/en-us/help/4598231
URL	https://support.microsoft.com/en-us/help/4598229
URL	https://support.microsoft.com/en-us/help/4598279
URL	https://support.microsoft.com/en-us/help/4598242
URL	https://support.microsoft.com/en-us/help/4598278
URL	https://support.microsoft.com/en-us/help/4598287
URL	https://support.microsoft.com/en-us/help/4598289

Type	Reference
URL	https://support.microsoft.com/en-us/help/4598288
URL	https://support.microsoft.com/en-us/help/4598245
URL	https://support.microsoft.com/en-us/help/4598285
URL	https://support.microsoft.com/en-us/help/4598243
URL	https://support.microsoft.com/en-us/help/4598297
URL	https://support.microsoft.com/en-us/help/4584787
URL	https://support.microsoft.com/en-us/help/4598275
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1697
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1710
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1663
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1669
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1686
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1643
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1649
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1700
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1695
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1658
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1678

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1690
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1650
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1659
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1662
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1648
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1638
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1706
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1687
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1651
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1696
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1673
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1664
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1679
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1672
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1703
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-26870

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1677
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1668
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1676
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1671
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1655
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1647
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1689
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1646
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1666
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1656
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1692
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1680
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1665
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1654
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1723
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1704

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1725
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1644
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1681
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1660
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1652
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1709
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1694
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1642
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1674
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1708
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1637
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1683
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1702
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1667
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1685
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1693

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1670
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1684
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1691
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1645
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1661
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1699
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1701
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1682
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1653
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1657
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1688

MS21-JUL: Microsoft Windows Out-of-Band Security Update — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their July 2021 out-of-band Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Workarounds:
Determine if the Print Spooler service is running:

Get-Service -Name Spooler

If the Print Spooler is running or if the service is not set to disabled, select one of the following options to either disable the Print Spooler service, or to Disable inbound remote printing through Group Policy:

Option 1 - Disable the Print Spooler service

If disabling the Print Spooler service is appropriate for your enterprise, use the following PowerShell commands:
Stop-Service -Name Spooler -Force
Set-Service -Name Spooler -StartupType Disabled

Impact of workaround: Disabling the Print Spooler service disables the ability to print both locally and remotely.

Option 2 - Disable inbound remote printing through Group Policy

Configure the settings via Group Policy as follows:
Computer Configuration / Administrative Templates / Printers
Disable the “Allow Print Spooler to accept client connections:” policy to block remote attacks.
You must restart the Print Spooler service for the group policy to take effect.

Impact of workaround This policy will block the remote attack vector by preventing inbound remote printing operations. The system will no longer function as a print server, but local printing to a directly attached device will still be possible.

Vulnerability Details

Remote code execution exploit in the Windows Print Spooler service known as “PrintNightmare”.

Microsoft has released a security update which includes fixes for the following vulnerability:

CVE-2021-34527 - Windows Print Spooler Remote Code Execution Vulnerability

Affected Products:
Windows 7 for x64-based Systems Service Pack 1
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows 8.1 for x64-based systems
Windows 8.1 for 32-bit systems
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows Server 2019 (Server Core installation)
Windows Server 2019

Windows 10 for x64-based Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems

https://support.microsoft.com/en-us/topic/july-6-2021-kb5004951-security-only-update-out-of-band-e05a81cd-9b45-4622-b715-ddb2367bca47
Impact:
An attacker who successfully exploited this vulnerability could run arbitrary code with SYSTEM privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

CVSS Base Score: 9

CVSS Vector: AV:N/AC:L/Au:S/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34527
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527
URL	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

MS21-JUL: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-31183 - Windows TCP/IP Driver Denial of Service Vulnerability
CVE-2021-31947 - HEVC Video Extensions Remote Code Execution Vulnerability

CVE-2021-31961 - Windows InstallService Elevation of Privilege Vulnerability
CVE-2021-31984 - Power BI Remote Code Execution Vulnerability
CVE-2021-33740 - Windows Media Remote Code Execution Vulnerability
CVE-2021-33743 - Windows Projected File System Elevation of Privilege Vulnerability
CVE-2021-33744 - Windows Secure Kernel Mode Security Feature Bypass Vulnerability
CVE-2021-33753 - Microsoft Bing Search Spoofing Vulnerability
CVE-2021-33755 - Windows Hyper-V Denial of Service Vulnerability
CVE-2021-33757 - Windows Security Account Manager Remote Protocol Security Feature Bypass Vulnerability
CVE-2021-33758 - Windows Hyper-V Denial of Service Vulnerability
CVE-2021-33759 - Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2021-33760 - Media Foundation Information Disclosure Vulnerability
CVE-2021-33761 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2021-33763 - Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2021-33765 - Windows Installer Spoofing Vulnerability
CVE-2021-33767 - Open Enclave SDK Elevation of Privilege Vulnerability
CVE-2021-33771 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-33773 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2021-33774 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-33780 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-34441 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2021-34442 - Windows DNS Server Denial of Service Vulnerability
CVE-2021-34491 - Win32k Information Disclosure Vulnerability
CVE-2021-34492 - Windows Certificate Spoofing Vulnerability
CVE-2021-34493 - Windows Partition Management Driver Elevation of Privilege Vulnerability
CVE-2021-34444 - Windows DNS Server Denial of Service Vulnerability
CVE-2021-34494 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-34445 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2021-34446 - Windows HTML Platforms Security Feature Bypass Vulnerability
CVE-2021-34496 - Windows GDI Information Disclosure Vulnerability
CVE-2021-34447 - Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2021-34497 - Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2021-34448 - Scripting Engine Memory Corruption Vulnerability
CVE-2021-34498 - Windows GDI Elevation of Privilege Vulnerability
CVE-2021-34449 - Win32k Elevation of Privilege Vulnerability
CVE-2021-34499 - Windows DNS Server Denial of Service Vulnerability
CVE-2021-34450 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2021-34500 - Windows Kernel Memory Information Disclosure Vulnerability
CVE-2021-34521 - Raw Image Extension Remote Code Execution Vulnerability
CVE-2021-34474 - Dynamics Business Central Remote Code Execution Vulnerability
CVE-2021-34476 - Bowser.sys Denial of Service Vulnerability
CVE-2021-34528 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-34479 - Microsoft Visual Studio Spoofing Vulnerability
CVE-2021-31979 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-33745 - Windows DNS Server Denial of Service Vulnerability
CVE-2021-33746 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-33749 - Windows DNS Snap-in Remote Code Execution Vulnerability
CVE-2021-33750 - Windows DNS Snap-in Remote Code Execution Vulnerability
CVE-2021-33751 - Storage Spaces Controller Elevation of Privilege Vulnerability

CVE-2021-33752 - Windows DNS Snap-in Remote Code Execution Vulnerability
CVE-2021-33754 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-33756 - Windows DNS Snap-in Remote Code Execution Vulnerability
CVE-2021-33764 - Windows Key Distribution Center Information Disclosure Vulnerability
CVE-2021-33772 - Windows TCP/IP Driver Denial of Service Vulnerability
CVE-2021-33775 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-33776 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-33777 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-33778 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-33779 - Windows ADFS Security Feature Bypass Vulnerability
CVE-2021-33781 - Active Directory Security Feature Bypass Vulnerability
CVE-2021-33782 - Windows Authenticode Spoofing Vulnerability
CVE-2021-33783 - Windows SMB Information Disclosure Vulnerability
CVE-2021-33784 - Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2021-33785 - Windows AF_UNIX Socket Provider Denial of Service Vulnerability
CVE-2021-33786 - Windows LSA Security Feature Bypass Vulnerability
CVE-2021-33788 - Windows LSA Denial of Service Vulnerability
CVE-2021-34438 - Windows Font Driver Host Remote Code Execution Vulnerability
CVE-2021-34439 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2021-34488 - Windows Console Driver Elevation of Privilege Vulnerability
CVE-2021-34489 - DirectWrite Remote Code Execution Vulnerability
CVE-2021-34440 - GDI+ Information Disclosure Vulnerability
CVE-2021-34490 - Windows TCP/IP Driver Denial of Service Vulnerability
CVE-2021-34503 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2021-34454 - Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2021-34504 - Windows Address Book Remote Code Execution Vulnerability
CVE-2021-34455 - Windows File History Service Elevation of Privilege Vulnerability
CVE-2021-34456 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2021-34457 - Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2021-34507 - Windows Remote Assistance Information Disclosure Vulnerability
CVE-2021-34458 - Windows Kernel Remote Code Execution Vulnerability
CVE-2021-34508 - Windows Kernel Remote Code Execution Vulnerability
CVE-2021-34459 - Windows AppContainer Elevation Of Privilege Vulnerability
CVE-2021-34509 - Storage Spaces Controller Information Disclosure Vulnerability
CVE-2021-34460 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-34510 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-34511 - Windows Installer Elevation of Privilege Vulnerability
CVE-2021-34461 - Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
CVE-2021-34512 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-34462 - Windows AppX Deployment Extensions Elevation of Privilege Vulnerability
CVE-2021-34513 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-34514 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-34464 - Microsoft Defender Remote Code Execution Vulnerability
CVE-2021-34516 - Win32k Elevation of Privilege Vulnerability
CVE-2021-34466 - Windows Hello Security Feature Bypass Vulnerability
CVE-2021-34522 - Microsoft Defender Remote Code Execution Vulnerability
CVE-2021-34525 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-34527 - Windows Print Spooler Remote Code Execution Vulnerability
CVE-2021-34477 - Visual Studio Code .NET Runtime Elevation of Privilege Vulnerability

CVE-2021-34529 - Visual Studio Code Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
HEVC Video Extensions
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Windows Server 2019
.NET Install Tool for Extension Authors
Windows 8.1 for x64-based systems
Microsoft Dynamics 365 Business Central 2021 Release Wave 1 - Update 18.3
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Microsoft Dynamics 365 Business Central 2020 Release Wave 1 - Update 16.14
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server, version 2004 (Server Core installation)
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Microsoft Malware Protection Engine
Windows Server 2012
Open Enclave SDK
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Microsoft Dynamics 365 Business Central 2020 Release Wave 2 - Update 17.8
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Microsoft Bing Search for Android
Windows 8.1 for 32-bit systems
Windows Server, version 1909 (Server Core installation)
.NET Education Bundle SDK Install Tool
Power BI Report Server
Windows 10 Version 1909 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1

Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their July 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 9.9

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33763
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34508
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34509
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34479
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34498
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33786
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33756
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33761
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34447
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33788
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34445
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33754
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33740
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34439
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34507

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34493
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33757
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33751
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34448
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34457
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34521
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34440
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34477
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31183
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33767
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34456
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34461
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34528
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34510
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34455
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34492
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34474
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34511
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33773
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34527
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34494
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33776
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33745
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33771

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33774
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33783
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34442
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33743
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31947
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34525
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33775
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34438
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31984
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33749
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34476
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33772
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33759
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34504
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34462
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34522
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34500
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31961
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34503
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33765
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34466
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34529
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34444
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33753

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34458
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33779
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33784
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33777
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33755
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34496
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33744
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34489
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33752
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34514
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33760
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34460
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33778
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34513
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33780
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33781
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34516
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34497
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33758
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34464
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33750
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34512
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34450
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33785

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34490
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34488
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34499
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34441
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34459
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33746
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31979
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33782
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34446
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34491
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34454
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33764
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34449
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34527
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33776
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33745
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33774
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33771
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33783
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34442

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33743
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31947
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34525
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33775
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34438
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31984
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33749
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34476
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33772
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33759
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34462
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34504
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34522
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34500
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34503
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31961

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34529
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34466
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33765
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34444
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33753
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34458
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33779
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33784
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33777
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33755
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34496
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33744
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34489
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34514
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33752
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34460

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33760
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34513
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33778
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34516
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33781
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33780
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34497
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33758
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34494
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34464
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33750
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34512
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34450
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33785
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34490
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34488

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34499
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34441
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34459
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33746
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31979
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33782
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34446
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34491
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34454
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33764
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34449
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34508
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33763
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34509
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33786
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34498

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34479
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33788
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34447
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33761
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33756
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34445
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33754
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34507
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34439
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33740
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34493
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33757
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33751
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34457
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34448
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34440

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34521
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34477
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34461
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34456
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33767
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31183
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34510
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34528
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34455
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34492
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34474
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-34511
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33773
URL	https://support.microsoft.com/en-us/help/5004238
URL	https://support.microsoft.com/en-us/help/5004955
URL	https://support.microsoft.com/en-us/help/5004954
URL	https://support.microsoft.com/en-us/help/5004237
URL	https://support.microsoft.com/en-us/help/5004299

Type	Reference
URL	https://support.microsoft.com/en-us/help/5004249
URL	https://support.microsoft.com/en-us/help/5004298
URL	https://support.microsoft.com/en-us/help/5004307
URL	https://support.microsoft.com/en-us/help/5004302
URL	https://support.microsoft.com/en-us/help/5004294
URL	https://support.microsoft.com/en-us/help/5004947
URL	https://support.microsoft.com/en-us/help/5004717
URL	https://support.microsoft.com/en-us/help/5004945
URL	https://support.microsoft.com/en-us/help/5004960
URL	https://support.microsoft.com/en-us/help/5004285
URL	https://support.microsoft.com/en-us/help/5004953
URL	https://support.microsoft.com/en-us/help/5004245
URL	https://support.microsoft.com/en-us/help/5004950
URL	https://support.microsoft.com/en-us/help/5004948
URL	https://support.microsoft.com/en-us/help/5004956
URL	https://support.microsoft.com/en-us/help/5004958
URL	https://support.microsoft.com/en-us/help/5004305
URL	https://support.microsoft.com/en-us/help/5004951
URL	https://support.microsoft.com/en-us/help/5004715
URL	https://support.microsoft.com/en-us/help/5004946
URL	https://support.microsoft.com/en-us/help/5004244
URL	https://support.microsoft.com/en-us/help/5004716
URL	https://support.microsoft.com/en-us/help/5004289

Type	Reference
URL	https://support.microsoft.com/en-us/help/5004959
URL	https://support.microsoft.com/en-us/help/5004233

MS21-JUN: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their June 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-1675 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-26414 - Windows DCOM Server Security Feature Bypass
CVE-2021-31938 - Microsoft VsCode Kubernetes Tools Extension Elevation of Privilege Vulnerability
CVE-2021-31942 - 3D Viewer Remote Code Execution Vulnerability
CVE-2021-31943 - 3D Viewer Remote Code Execution Vulnerability
CVE-2021-31944 - 3D Viewer Information Disclosure Vulnerability
CVE-2021-31945 - Paint 3D Remote Code Execution Vulnerability
CVE-2021-31946 - Paint 3D Remote Code Execution Vulnerability
CVE-2021-31951 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-31952 - Windows Kernel-Mode Driver Elevation of Privilege Vulnerability
CVE-2021-31953 - Windows Filter Manager Elevation of Privilege Vulnerability
CVE-2021-31954 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-31955 - Windows Kernel Information Disclosure Vulnerability
CVE-2021-31956 - Windows NTFS Elevation of Privilege Vulnerability
CVE-2021-31957 - .NET Core and Visual Studio Denial of Service Vulnerability
CVE-2021-31958 - Windows NTLM Elevation of Privilege Vulnerability
CVE-2021-31959 - Scripting Engine Memory Corruption Vulnerability
CVE-2021-31960 - Windows Bind Filter Driver Information Disclosure Vulnerability
CVE-2021-31962 - Kerberos AppContainer Security Feature Bypass Vulnerability
CVE-2021-31967 - VP9 Video Extensions Remote Code Execution Vulnerability
CVE-2021-31980 - Microsoft Intune Management Extension Remote Code Execution Vulnerability
CVE-2021-31983 - Paint 3D Remote Code Execution Vulnerability
CVE-2021-33739 - Microsoft DWM Core Library Elevation of Privilege Vulnerability
CVE-2021-33742 - Windows MSHTML Platform Remote Code Execution Vulnerability
CVE-2021-31199 - Microsoft Enhanced Cryptographic Provider Elevation of Privilege Vulnerability
CVE-2021-31201 - Microsoft Enhanced Cryptographic Provider Elevation of Privilege Vulnerability
CVE-2021-31968 - Windows Remote Desktop ServicesÂ Denial of Service Vulnerability

CVE-2021-31969 - Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2021-31970 - Windows TCP/IP Driver Security Feature Bypass Vulnerability
CVE-2021-31971 - Windows HTML Platform Security Feature Bypass Vulnerability
CVE-2021-31972 - Event Tracing for Windows Information Disclosure Vulnerability
CVE-2021-31973 - Windows GPSVC Elevation of Privilege Vulnerability
CVE-2021-31974 - Server for NFS Denial of Service Vulnerability
CVE-2021-31975 - Server for NFS Information Disclosure Vulnerability
CVE-2021-31976 - Server for NFS Information Disclosure Vulnerability
CVE-2021-31977 - Windows Hyper-V Denial of Service Vulnerability
CVE-2021-31978 - Microsoft Defender Denial of Service Vulnerability
CVE-2021-31985 - Microsoft Defender Remote Code Execution Vulnerability
CVE-2021-33741 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Paint 3D
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows Server, version 20H2 (Server Core Installation)
Intune management extension
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Microsoft Malware Protection Engine
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Microsoft Edge (Chromium-based)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
.NET 5.0
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Microsoft Visual Studio 2019 version 16.10 (includes 16.0 - 16.9)
Visual Studio 2019 for Mac version 8.10
Windows 10 Version 20H2 for ARM64-based Systems
.NET Core 3.1
Windows 10 Version 1909 for x64-based Systems
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Windows 10 Version 1909 for ARM64-based Systems
Visual Studio Code - Kubernetes Tools
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)

Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
VP9 Video Extensions
Windows Server, version 2004 (Server Core installation)
Windows Server 2019 (Server Core installation)
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
3D Viewer
Windows 10 Version 21H1 for ARM64-based Systems

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33741
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31959
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31983
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31967
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33739
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31974
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31943
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1675
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31958
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31944
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31945
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31951
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31985

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31946
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31955
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31954
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31980
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31938
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31975
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31199
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31962
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33742
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31956
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31968
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31942
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31201
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31973
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31976
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31978
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31957
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31970
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31953
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31952
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31960
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31971
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31969

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26414
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31977
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31972
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31959
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31983
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31967
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33739
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31974
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31943
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1675
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31958
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31944
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31945
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31951
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31985
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31946
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31955

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31980
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31938
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31954
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31975
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31199
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31962
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33742
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31956
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31968
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31942
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-33741
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31201
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31973
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31976
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31978
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31957

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31953
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31952
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31960
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31970
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31969
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31971
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26414
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31977
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31972
URL	https://support.microsoft.com/en-us/help/5003697
URL	https://support.microsoft.com/en-us/help/5003671
URL	https://support.microsoft.com/en-us/help/5003694
URL	https://support.microsoft.com/en-us/help/5003635
URL	https://support.microsoft.com/en-us/help/5003661
URL	https://support.microsoft.com/en-us/help/5003681
URL	https://support.microsoft.com/en-us/help/5003638
URL	https://support.microsoft.com/en-us/help/5003695
URL	https://support.microsoft.com/en-us/help/5003636
URL	https://support.microsoft.com/en-us/help/5003667
URL	https://support.microsoft.com/en-us/help/5003687

Type	Reference
URL	https://support.microsoft.com/en-us/help/5003696
URL	https://support.microsoft.com/en-us/help/5003646
URL	https://support.microsoft.com/en-us/help/5003637

MS21-MAR: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their March 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2021-26411 - Internet Explorer Memory Corruption Vulnerability
CVE-2021-27085 - Internet Explorer Remote Code Execution Vulnerability

Affected Products:
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 20H2 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1903 for ARM64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 20H2 for x64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for ARM64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 20H2 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1903 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows Server 2016

Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 2004 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 20H2 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1803 for ARM64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 20H2 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows Server 2019
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2012
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 2004 for 32-bit Systems
Microsoft Edge (EdgeHTML-based) on Windows 10 Version 1607 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 20H2 for 32-bit Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26411
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27085
URL	https://support.microsoft.com/en-us/help/5000822
URL	https://support.microsoft.com/en-us/help/5000803

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27085
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26411
URL	https://support.microsoft.com/en-us/help/5000802
URL	https://support.microsoft.com/en-us/help/5000809
URL	https://support.microsoft.com/en-us/help/5000847
URL	https://support.microsoft.com/en-us/help/5000807
URL	https://support.microsoft.com/en-us/help/5000841
URL	https://support.microsoft.com/en-us/help/5000808
URL	https://support.microsoft.com/en-us/help/5000848
URL	https://support.microsoft.com/en-us/help/5000800
URL	https://support.microsoft.com/en-us/help/5000844

MS21-MAR: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their March 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-1640 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-1729 - Windows Update Stack Setup Elevation of Privilege Vulnerability
CVE-2021-24095 - DirectX Elevation of Privilege Vulnerability
CVE-2021-27060 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-27070 - Windows 10 Update Assistant Elevation of Privilege Vulnerability
CVE-2021-27074 - Azure Sphere Unsigned Code Execution Vulnerability
CVE-2021-27075 - Azure Virtual Machine Information Disclosure Vulnerability

CVE-2021-27077 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-27080 - Azure Sphere Unsigned Code Execution Vulnerability
CVE-2021-27081 - Visual Studio Code ESLint Extension Remote Code Execution Vulnerability
CVE-2021-27082 - Quantum Development Kit for Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-27083 - Remote Development Extension for Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-24089 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-24090 - Windows Error Reporting Elevation of Privilege Vulnerability
CVE-2021-24107 - Windows Event Tracing Information Disclosure Vulnerability
CVE-2021-24110 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-26859 - Microsoft Power BI Information Disclosure Vulnerability
CVE-2021-26860 - Windows App-V Overlay Filter Elevation of Privilege Vulnerability
CVE-2021-26861 - Windows Graphics Component Remote Code Execution Vulnerability
CVE-2021-26862 - Windows Installer Elevation of Privilege Vulnerability
CVE-2021-26863 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-26864 - Windows Virtual Registry Provider Elevation of Privilege Vulnerability
CVE-2021-26865 - Windows Container Execution Agent Elevation of Privilege Vulnerability
CVE-2021-26866 - Windows Update Service Elevation of Privilege Vulnerability
CVE-2021-26867 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2021-26868 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2021-26869 - Windows ActiveX Installer Service Information Disclosure Vulnerability
CVE-2021-26870 - Windows Projected File System Elevation of Privilege Vulnerability
CVE-2021-26871 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-26872 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-26873 - Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2021-26874 - Windows Overlay Filter Elevation of Privilege Vulnerability
CVE-2021-26875 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-26876 - OpenType Font Parsing Remote Code Execution Vulnerability
CVE-2021-26877 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-26878 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-26879 - Windows NAT Denial of Service Vulnerability
CVE-2021-26880 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-26881 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2021-26882 - Remote Access API Elevation of Privilege Vulnerability
CVE-2021-26884 - Windows Media Photo Codec Information Disclosure Vulnerability
CVE-2021-26885 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-26886 - User Profile Service Denial of Service Vulnerability
CVE-2021-26887 - Microsoft Windows Folder Redirection Elevation of Privilege Vulnerability
CVE-2021-26889 - Windows Update Stack Elevation of Privilege Vulnerability
CVE-2021-26890 - Application Virtualization Remote Code Execution Vulnerability
CVE-2021-26891 - Windows Container Execution Agent Elevation of Privilege Vulnerability
CVE-2021-26892 - Windows Extensible Firmware Interface Security Feature Bypass Vulnerability
CVE-2021-26893 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-26894 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-26895 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-26896 - Windows DNS Server Denial of Service Vulnerability
CVE-2021-26897 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-26898 - Windows Event Tracing Elevation of Privilege Vulnerability

CVE-2021-26899 - Windows UPnP Device Host Elevation of Privilege Vulnerability
CVE-2021-26900 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2021-26901 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-26902 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-27047 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-27048 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-27049 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-27050 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-27051 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-27058 - Microsoft Office ClickToRun Remote Code Execution Vulnerability
CVE-2021-27061 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-27062 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-27063 - Windows DNS Server Denial of Service Vulnerability
CVE-2021-27066 - Windows Admin Center Security Feature Bypass Vulnerability
CVE-2021-21300 - Git for Visual Studio Remote Code Execution Vulnerability
CVE-2021-27084 - Visual Studio Code Java Extension Pack Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
HEVC Video Extensions
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Microsoft Quantum Development Kit for Visual Studio Code
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Microsoft 365 Apps for Enterprise for 64-bit Systems
Windows Server 2019
Windows 10 Version 1803 for x64-based Systems
Windows 8.1 for x64-based systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Power BI Report Server version 15.0.1103.234
Microsoft Visual Studio 2019 version 16.8 (includes 16.0 - 16.7)
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Visual Studio Code Remote - Containers Extension
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server, version 2004 (Server Core installation)

Azure Container Instance
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Azure Sphere
Azure Spring Cloud
Windows 10 Version 1809 for x64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Windows Admin Center
Microsoft 365 Apps for Enterprise for 32-bit Systems
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Azure Kubernetes Service
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Azure Service Fabric
Windows Server, version 1909 (Server Core installation)
Power BI Report Server version 15.0.1104.300
Visual Studio Code - Java Extension Pack
Microsoft Visual Studio Code ESLint extension
Windows 10 Version 1909 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1640
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26887
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26877
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26902
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27077
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26871

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26882
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24090
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24089
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27051
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26894
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26889
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26895
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27084
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27047
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27081
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26879
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26891
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26859
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26872
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26860
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27075
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27080
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26901
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26868
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27063
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27070
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26867
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27062
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24107

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27058
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26873
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26869
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26870
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26874
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26896
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27066
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27060
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24095
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26885
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26864
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-24110
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27061
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26862
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26880
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26892
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26865
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26899
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26861
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26881
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26863
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27050
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27049
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26893

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27082
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26900
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27048
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26876
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26884
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21300
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1729
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26878
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26875
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26890
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26886
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26898
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26897
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26866
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27083
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27074
URL	https://support.microsoft.com/en-us/help/5000809
URL	https://support.microsoft.com/en-us/help/5000803
URL	https://support.microsoft.com/en-us/help/5000841
URL	https://support.microsoft.com/en-us/help/5000808
URL	https://support.microsoft.com/en-us/help/5000802
URL	https://support.microsoft.com/en-us/help/5001285
URL	https://support.microsoft.com/en-us/help/5000840
URL	https://support.microsoft.com/en-us/help/5000856

Type	Reference
URL	https://support.microsoft.com/en-us/help/5001284
URL	https://support.microsoft.com/en-us/help/5000853
URL	https://support.microsoft.com/en-us/help/5000851
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27060
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24095
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26885
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26864
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24110
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27061
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26862
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26892
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26865
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26899
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26861
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26881
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26863
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27050

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27049
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26893
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27082
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26900
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26896
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26874
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26870
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26879
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27081
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26886
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27080
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26890
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26898
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26897
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27084
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26895

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27047
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26875
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-21300
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1729
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26878
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26884
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26876
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27048
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27074
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27083
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26866
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26869
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26873
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27058
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24107
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27062

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26867
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27070
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27063
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26868
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26901
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27075
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26860
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26872
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26859
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26891
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26889
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26880
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26894
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27051
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24089
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-24090

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26882
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27077
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26871
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26902
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26877
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26887
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1640
URL	https://support.microsoft.com/en-us/help/5000822
URL	https://support.microsoft.com/en-us/help/5000844
URL	https://support.microsoft.com/en-us/help/5000848
URL	https://support.microsoft.com/en-us/help/5000847
URL	https://support.microsoft.com/en-us/help/5000807
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27066

MS21-MAY: Microsoft Internet Explorer Security Update High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their May 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2021-26419 - Scripting Engine Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 2004 for ARM64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 20H2 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 2004 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1909 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 20H2 for ARM64-based Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2012
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 2004 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 20H2 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1909 for 32-bit Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26419
URL	https://support.microsoft.com/en-us/help/5003233
URL	https://support.microsoft.com/en-us/help/5003174

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26419
URL	https://support.microsoft.com/en-us/help/5003208
URL	https://support.microsoft.com/en-us/help/5003173
URL	https://support.microsoft.com/en-us/help/5003165
URL	https://support.microsoft.com/en-us/help/5003209
URL	https://support.microsoft.com/en-us/help/5003210
URL	https://support.microsoft.com/en-us/help/5003197
URL	https://support.microsoft.com/en-us/help/5003172
URL	https://support.microsoft.com/en-us/help/5003171
URL	https://support.microsoft.com/en-us/help/5003169

MS21-MAY: Microsoft Windows Security Update — High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2020-24588 - Windows Wireless Networking Spoofing Vulnerability
CVE-2020-24587 - Windows Wireless Networking Information Disclosure Vulnerability
CVE-2021-27068 - Visual Studio Remote Code Execution Vulnerability
CVE-2020-26144 - Windows Wireless Networking Spoofing Vulnerability
CVE-2021-28461 - Dynamics Finance and Operations Cross-site Scripting Vulnerability
CVE-2021-28479 - Windows CSC Service Information Disclosure Vulnerability
CVE-2021-31165 - Windows Container Manager Service Elevation of Privilege Vulnerability
CVE-2021-31166 - HTTP Protocol Stack Remote Code Execution Vulnerability
CVE-2021-31167 - Windows Container Manager Service Elevation of Privilege Vulnerability
CVE-2021-31168 - Windows Container Manager Service Elevation of Privilege Vulnerability
CVE-2021-31169 - Windows Container Manager Service Elevation of Privilege Vulnerability
CVE-2021-31170 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2021-31182 - Microsoft Bluetooth Driver Spoofing Vulnerability
CVE-2021-31184 - Microsoft Windows Infrared Data Association (IrDA) Information Disclosure Vulnerability
CVE-2021-31185 - Windows Desktop Bridge Denial of Service Vulnerability
CVE-2021-31186 - Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
CVE-2021-31187 - Windows WalletService Elevation of Privilege Vulnerability
CVE-2021-31188 - Windows Graphics Component Elevation of Privilege Vulnerability

CVE-2021-31190 - Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
CVE-2021-31191 - Windows Projected File System FS Filter Driver Information Disclosure Vulnerability
CVE-2021-31192 - Windows Media Foundation Core Remote Code Execution Vulnerability
CVE-2021-31193 - Windows SSDP Service Elevation of Privilege Vulnerability
CVE-2021-31194 - OLE Automation Remote Code Execution Vulnerability
CVE-2021-31204 - .NET and Visual Studio Elevation of Privilege Vulnerability
CVE-2021-31205 - Windows SMB Client Security Feature Bypass Vulnerability
CVE-2021-31208 - Windows Container Manager Service Elevation of Privilege Vulnerability
CVE-2021-31211 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-31213 - Visual Studio Code Remote Containers Extension Remote Code Execution Vulnerability
CVE-2021-31214 - Visual Studio Code Remote Code Execution Vulnerability
CVE-2021-28465 - Web Media Extensions Remote Code Execution Vulnerability
CVE-2021-28476 - Hyper-V Remote Code Execution Vulnerability
CVE-2021-31200 - Common Utilities Remote Code Execution Vulnerability
CVE-2021-31936 - Microsoft Accessibility Insights for Web Information Disclosure Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows Server, version 20H2 (Server Core Installation)
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Dynamics 365 for Finance and Operations
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Windows 10 Version 1803 for x64-based Systems
common_utils.py
.NET 5.0
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows Server, version 1909 (Server Core installation)
.NET Core 3.1
Windows 10 Version 1909 for x64-based Systems
Microsoft Accessibility Insights for Web
Visual Studio 2019 for Mac version 8.9
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Visual Studio Code Remote - Containers Extension
Windows 10 Version 1909 for ARM64-based Systems

Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Web Media Extensions
Windows 10 Version 2004 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1803 for ARM64-based Systems
Windows Server, version 2004 (Server Core installation)
Windows Server 2019 (Server Core installation)
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their May 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 9.9

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31211
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-27068
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31213
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28476
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31188
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31165
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-24588

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31182
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31205
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31191
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28479
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31167
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31190
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31208
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31169
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31166
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31185
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28465
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31936
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31214
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31186
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31204
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28461
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31193
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-26144
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31194
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-24587
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31192
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31184
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31170
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31187

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31168
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-31200
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31193
URL	https://support.microsoft.com/en-us/help/5003174
URL	https://support.microsoft.com/en-us/help/5003233
URL	https://support.microsoft.com/en-us/help/5003169
URL	https://support.microsoft.com/en-us/help/5003171
URL	https://support.microsoft.com/en-us/help/5003172
URL	https://support.microsoft.com/en-us/help/5003197
URL	https://support.microsoft.com/en-us/help/5003210
URL	https://support.microsoft.com/en-us/help/5003209
URL	https://support.microsoft.com/en-us/help/5003173
URL	https://support.microsoft.com/en-us/help/5003208
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31211
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28476
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31213
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-27068
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31188
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31165
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-24588

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31182
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31205
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31191
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28479
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31167
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31190
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31208
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31169
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31166
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31185
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28465
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31936
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31214
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31186
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31204
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-28461

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-26144
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31194
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-24587
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31192
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31184
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31170
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31187
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31168
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-31200
URL	https://support.microsoft.com/en-us/help/5003220
URL	https://support.microsoft.com/en-us/help/5003203
URL	https://support.microsoft.com/en-us/help/5003228
URL	https://support.microsoft.com/en-us/help/5003225
URL	https://github.com/vanhoefm/fragattacks/blob/master/SUMMARY.md

MS21-NOV: Microsoft Windows Security Update — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their November 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-36957 - Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2021-38631 - Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
CVE-2021-3711 - OpenSSL: CVE-2021-3711 SM2 Decryption Buffer Overflow
CVE-2021-41366 - Credential Security Support Provider Protocol (CredSSP) Elevation of Privilege Vulnerability
CVE-2021-41367 - NTFS Elevation of Privilege Vulnerability
CVE-2021-41371 - Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
CVE-2021-41372 - Power BI Report Server Spoofing Vulnerability
CVE-2021-41377 - Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
CVE-2021-41378 - Windows NTFS Remote Code Execution Vulnerability
CVE-2021-41379 - Windows Installer Elevation of Privilege Vulnerability
CVE-2021-26443 - Microsoft Virtual Machine Bus (VMBus) Remote Code Execution Vulnerability
CVE-2021-42274 - Windows Hyper-V Discrete Device Assignment (DDA) Denial of Service Vulnerability
CVE-2021-42275 - Microsoft COM for Windows Remote Code Execution Vulnerability
CVE-2021-42276 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2021-42278 - Active Directory Domain Services Elevation of Privilege Vulnerability
CVE-2021-42279 - Chakra Scripting Engine Memory Corruption Vulnerability
CVE-2021-42280 - Windows Feedback Hub Elevation of Privilege Vulnerability
CVE-2021-42300 - Azure Sphere Tampering Vulnerability
CVE-2021-42301 - Azure RTOS Information Disclosure Vulnerability
CVE-2021-42302 - Azure RTOS Elevation of Privilege Vulnerability
CVE-2021-42303 - Azure RTOS Elevation of Privilege Vulnerability
CVE-2021-42304 - Azure RTOS Elevation of Privilege Vulnerability
CVE-2021-42316 - Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability
CVE-2021-42319 - Visual Studio Elevation of Privilege Vulnerability
CVE-2021-42322 - Visual Studio Code Elevation of Privilege Vulnerability
CVE-2021-43208 - 3D Viewer Remote Code Execution Vulnerability
CVE-2021-43209 - 3D Viewer Remote Code Execution Vulnerability
CVE-2021-38665 - Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2021-38666 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2021-41351 - Microsoft Edge (Chrome based) Spoofing on IE Mode
CVE-2021-41356 - Windows Denial of Service Vulnerability
CVE-2021-41370 - NTFS Elevation of Privilege Vulnerability
CVE-2021-41373 - FSLogix Information Disclosure Vulnerability
CVE-2021-41374 - Azure Sphere Information Disclosure Vulnerability
CVE-2021-41375 - Azure Sphere Information Disclosure Vulnerability
CVE-2021-41376 - Azure Sphere Information Disclosure Vulnerability
CVE-2021-42277 - Diagnostics Hub Standard Collector Elevation of Privilege Vulnerability
CVE-2021-42282 - Active Directory Domain Services Elevation of Privilege Vulnerability
CVE-2021-42283 - NTFS Elevation of Privilege Vulnerability
CVE-2021-42284 - Windows Hyper-V Denial of Service Vulnerability
CVE-2021-42285 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-42286 - Windows Core Shell SI Host Extension Framework for Composable Shell Elevation of Privilege Vulnerability
CVE-2021-42287 - Active Directory Domain Services Elevation of Privilege Vulnerability

CVE-2021-42288 - Windows Hello Security Feature Bypass Vulnerability
CVE-2021-42291 - Active Directory Domain Services Elevation of Privilege Vulnerability
CVE-2021-42298 - Microsoft Defender Remote Code Execution Vulnerability
CVE-2021-42323 - Azure RTOS Information Disclosure Vulnerability
CVE-2021-26444 - Azure RTOS Information Disclosure Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Windows Server 2022 (Server Core installation)
Windows Server 2019
Microsoft Edge (Chromium-based) in IE Mode on Windows 11 for x64-based Systems
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 1909 for 32-bit Systems
Windows 8.1 for x64-based systems
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 11 for x64-based Systems
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Azure RTOS
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Remote Desktop client for Windows Desktop
Microsoft Dynamics 365 (on-premises) version 9.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 2004 for ARM64-based Systems
Microsoft Visual Studio 2015 Update 3
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Edge (Chromium-based) in IE Mode on Windows Server 2019
Windows Server, version 2004 (Server Core installation)
Azure Sphere
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows 10 Version 1809 for x64-based Systems
3D Viewer
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 21H1 for ARM64-based Systems
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 1809 for x64-based Systems
Windows Server, version 20H2 (Server Core Installation)

Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 21H1 for x64-based Systems
Microsoft Malware Protection Engine
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 20H2 for ARM64-based Systems
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 1809 for 32-bit Systems
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 2004 for ARM64-based Systems
Windows Server 2022
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Microsoft Edge (Chromium-based) in IE Mode on Windows 11 for ARM64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 21H1 for ARM64-based Systems
Windows Server 2012 R2 (Server Core installation)
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 1809 for ARM64-based Systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 2004 for 32-bit Systems
Power BI Report Server
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 20H2 for x64-based Systems
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 2004 for x64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Windows 11 for ARM64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Microsoft Edge (Chromium-based) in IE Mode on Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
FSLogix

CVSS Base Score: 9.6

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41378
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42278
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41371
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42275

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42283
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26444
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42304
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38631
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41372
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41351
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41375
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42284
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42276
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41373
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41374
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43208
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42303
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42300
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41367
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42322
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36957
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42291
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42280
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42298
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42302
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41356
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43209
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42282

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42319
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42285
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41366
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42316
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42301
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42287
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38665
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41370
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41377
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42277
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42279
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42274
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41379
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42288
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38666
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41376
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26443
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42286
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-42323
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-3711
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-3711
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42316
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42287

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42301
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38665
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42277
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41377
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41379
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42274
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42279
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42288
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38666
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41376
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42286
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26443
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42323
URL	https://support.microsoft.com/en-us/help/5008479
URL	https://support.microsoft.com/en-us/help/5007205
URL	https://support.microsoft.com/en-us/help/5007275
URL	https://support.microsoft.com/en-us/help/5007246
URL	https://support.microsoft.com/en-us/help/5007207

Type	Reference
URL	https://support.microsoft.com/en-us/help/5007206
URL	https://support.microsoft.com/en-us/help/5007215
URL	https://support.microsoft.com/en-us/help/5007255
URL	https://support.microsoft.com/en-us/help/5007233
URL	https://support.microsoft.com/en-us/help/5007245
URL	https://support.microsoft.com/en-us/help/5007186
URL	https://support.microsoft.com/en-us/help/5007260
URL	https://support.microsoft.com/en-us/help/5007236
URL	https://support.microsoft.com/en-us/help/5007189
URL	https://support.microsoft.com/en-us/help/5007263
URL	https://support.microsoft.com/en-us/help/5008478
URL	https://support.microsoft.com/en-us/help/5007247
URL	https://support.microsoft.com/en-us/help/5007903
URL	https://support.microsoft.com/en-us/help/5007192
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41370
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42278
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41378
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41371
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42275
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42283

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26444
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42304
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38631
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41375
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41351
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41372
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42284
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42276
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41374
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41373
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43208
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42303
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42300
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42322
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41367
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42291

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36957
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42298
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42280
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42302
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41356
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-43209
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42282
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42319
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-42285
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41366

MS21-OCT: Microsoft Internet Explorer Security Update — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their October 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2021-41342 - Windows MSHTML Platform Remote Code Execution Vulnerability

Affected Products:
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Windows Server 2022
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 11 for x64-based Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 11 for ARM64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H1 for ARM64-based Systems

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41342
URL	https://support.microsoft.com/en-us/help/5006714
URL	https://support.microsoft.com/en-us/help/5006699
URL	https://support.microsoft.com/en-us/help/5006670

Type	Reference
URL	https://support.microsoft.com/en-us/help/5006669
URL	https://support.microsoft.com/en-us/help/5006671
URL	https://support.microsoft.com/en-us/help/5006674
URL	https://support.microsoft.com/en-us/help/5006743
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41342
URL	https://support.microsoft.com/en-us/help/5006739
URL	https://support.microsoft.com/en-us/help/5006667
URL	https://support.microsoft.com/en-us/help/5006672
URL	https://support.microsoft.com/en-us/help/5006675
URL	https://support.microsoft.com/en-us/help/5006736

MS21-OCT: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their October 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-36953 - Windows TCP/IP Denial of Service Vulnerability
CVE-2021-36970 - Windows Print Spooler Spoofing Vulnerability
CVE-2021-40443 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-40449 - Win32k Elevation of Privilege Vulnerability
CVE-2021-40455 - Windows Installer Spoofing Vulnerability
CVE-2021-40456 - Windows AD FS Security Feature Bypass Vulnerability
CVE-2021-40457 - Microsoft Dynamics 365 Customer Engagement Cross-Site Scripting Vulnerability
CVE-2021-40475 - Windows Cloud Files Mini Filter Driver Information Disclosure Vulnerability
CVE-2021-40476 - Windows AppContainer Elevation Of Privilege Vulnerability
CVE-2021-40477 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-40478 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-41355 - .NET Core and Visual Studio Information Disclosure Vulnerability
CVE-2021-41361 - Active Directory Federation Server Spoofing Vulnerability
CVE-2021-3450 - OpenSSL: CVE-2021-3450 CA certificate check bypass with X509_V_FLAG_X509_STRICT

CVE-2021-3449 - OpenSSL: CVE-2021-3449 NULL pointer deref in signature_algorithms processing
CVE-2020-1971 - OpenSSL: CVE-2020-1971 EDIPARTYNAME NULL pointer de-reference
CVE-2021-38662 - Windows Fast FAT File System Driver Information Disclosure Vulnerability
CVE-2021-38663 - Windows exFAT File System Information Disclosure Vulnerability
CVE-2021-38672 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2021-40450 - Win32k Elevation of Privilege Vulnerability
CVE-2021-40460 - Windows Remote Procedure Call Runtime Security Feature Bypass Vulnerability
CVE-2021-40461 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2021-40462 - Windows Media Foundation Dolby Digital Atmos Decoders Remote Code Execution Vulnerability
CVE-2021-40463 - Windows NAT Denial of Service Vulnerability
CVE-2021-40464 - Windows Nearby Sharing Elevation of Privilege Vulnerability
CVE-2021-40465 - Windows Text Shaping Remote Code Execution Vulnerability
CVE-2021-40466 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-40467 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-40468 - Windows Bind Filter Driver Information Disclosure Vulnerability
CVE-2021-40469 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2021-40470 - DirectX Graphics Kernel Elevation of Privilege Vulnerability
CVE-2021-40488 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-40489 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-26441 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-26442 - Windows HTTP.sys Elevation of Privilege Vulnerability
CVE-2021-41330 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2021-41331 - Windows Media Audio Decoder Remote Code Execution Vulnerability
CVE-2021-41332 - Windows Print Spooler Information Disclosure Vulnerability
CVE-2021-41334 - Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2021-41335 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-41336 - Windows Kernel Information Disclosure Vulnerability
CVE-2021-41337 - Active Directory Security Feature Bypass Vulnerability
CVE-2021-41338 - Windows AppContainer Firewall Rules Security Feature Bypass Vulnerability
CVE-2021-41339 - Microsoft DWM Core Library Elevation of Privilege Vulnerability
CVE-2021-41340 - Windows Graphics Component Remote Code Execution Vulnerability
CVE-2021-41343 - Windows Fast FAT File System Driver Information Disclosure Vulnerability
CVE-2021-41345 - Storage Spaces Controller Elevation of Privilege Vulnerability
CVE-2021-41346 - Console Window Host Security Feature Bypass Vulnerability
CVE-2021-41347 - Windows AppX Deployment Service Elevation of Privilege Vulnerability
CVE-2021-41352 - SCOM Information Disclosure Vulnerability
CVE-2021-41353 - Microsoft Dynamics 365 (on-premises) Spoofing Vulnerability
CVE-2021-41354 - Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability
CVE-2021-41357 - Win32k Elevation of Privilege Vulnerability
CVE-2021-37974 - Chromium: CVE-2021-37974 Use after free in Safe Browsing
CVE-2021-37975 - Chromium: CVE-2021-37975 Use after free in V8
CVE-2021-37976 - Chromium: CVE-2021-37976 Information leak in core
CVE-2021-41363 - Intune Management Extension Security Feature Bypass Vulnerability
CVE-2021-37977 - Chromium: CVE-2021-37977 Use after free in Garbage Collection
CVE-2021-37978 - Chromium: CVE-2021-37978 Heap buffer overflow in Blink
CVE-2021-37979 - Chromium: CVE-2021-37979 Heap buffer overflow in WebRTC
CVE-2021-37980 - Chromium: CVE-2021-37980 Inappropriate implementation in Sandbox

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
Windows Server, version 20H2 (Server Core Installation)
Intune management extension
System Center 2019 Operations Manager
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Microsoft Edge (Chromium-based)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
System Center 2012 R2 Operations Manager
.NET 5.0
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
System Center 2016 Operations Manager
Windows 8.1 for 32-bit systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 11 for x64-based Systems
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Windows 10 Version 2004 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 11 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems

Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Dynamics 365 Customer Engagement V9.1
Windows Server, version 2004 (Server Core installation)
Windows Server 2019 (Server Core installation)
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows Server 2016
Microsoft Dynamics 365 Customer Engagement V9.0
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows 10 Version 21H1 for ARM64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37976
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37975
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37974
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41363
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41361
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41335
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41357
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41347
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41354
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40478
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40449
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38662
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40463
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41338
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41331

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41353
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40455
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40466
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41339
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40477
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40467
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40456
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36953
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40488
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41352
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41345
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40469
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40461
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41334
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40443
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41343
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40450
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40465
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40462
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36970
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40468
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40489
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41332

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40464
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40470
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26441
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38672
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41336
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40460
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41346
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41330
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41340
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38663
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40457
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41355
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41337
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40476
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40475
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26442
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-3449
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-3450
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1971
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37978
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37977
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37980
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-37979
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40466

Type	Reference
URL	https://chromereleases.googleblog.com/2021/09/stable-channel-update-for-desktop_30.html
URL	https://support.microsoft.com/en-us/help/5006743
URL	https://support.microsoft.com/en-us/help/5006674
URL	https://support.microsoft.com/en-us/help/5006739
URL	https://support.microsoft.com/en-us/help/5006669
URL	https://support.microsoft.com/en-us/help/5006670
URL	https://support.microsoft.com/en-us/help/5006699
URL	https://support.microsoft.com/en-us/help/5006714
URL	https://support.microsoft.com/en-us/help/5006736
URL	https://support.microsoft.com/en-us/help/5006675
URL	https://support.microsoft.com/en-us/help/5006672
URL	https://support.microsoft.com/en-us/help/5006667
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41363
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-3449
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41361
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41335
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40468
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37978
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41357
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40489

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41332
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41347
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41354
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40464
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40478
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1971
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40449
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38662
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41338
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41331
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40470
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40463
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41353
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40455
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26441
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38672

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41339
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40477
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37975
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41336
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37977
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40467
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40460
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37980
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40456
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37974
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41346
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36953
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40488
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41352
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41345
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41330

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40469
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40461
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41340
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37976
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41334
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38663
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40457
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40443
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41343
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40450
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41355
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-41337
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40476
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40475
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26442
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40465

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40462
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-3450
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36970
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-37979
URL	https://support.microsoft.com/en-us/help/5006871
URL	https://support.microsoft.com/en-us/help/4618810
URL	https://support.microsoft.com/en-us/help/5006732
URL	https://support.microsoft.com/en-us/help/5006728
URL	https://support.microsoft.com/en-us/help/5006715
URL	https://support.microsoft.com/en-us/help/5006729
URL	https://git.openssl.org/gitweb/?p=openssl.git;a=commitdiff;h=2154ab83e14ede338d2ede9bbe5cdfce5d5a6c9e
URL	https://support.microsoft.com/en-us/help/4618795

MS21-SEP: Microsoft Internet Explorer Security Update High

Solution Details

Microsoft has released a fix for this flaw in their September 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2021-40444 - Microsoft MSHTML Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows Server, version 20H2 (Server Core Installation)
Windows 10 for 32-bit Systems

Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Windows Server 2022
Windows Server 2022 (Server Core installation)
Windows Server 2019
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows RT 8.1
Windows 10 Version 2004 for ARM64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows Server, version 2004 (Server Core installation)
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows 10 Version 21H1 for ARM64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40444

Type	Reference
URL	https://support.microsoft.com/en-us/help/5005563
URL	https://support.microsoft.com/en-us/help/5005573
URL	https://support.microsoft.com/en-us/help/5005627
URL	https://support.microsoft.com/en-us/help/5005606
URL	https://support.microsoft.com/en-us/help/5005575
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40444
URL	https://support.microsoft.com/en-us/help/5005565
URL	https://support.microsoft.com/en-us/help/5005569
URL	https://support.microsoft.com/en-us/help/5005568
URL	https://support.microsoft.com/en-us/help/5005633
URL	https://support.microsoft.com/en-us/help/5005613
URL	https://support.microsoft.com/en-us/help/5005623
URL	https://support.microsoft.com/en-us/help/5005566

MS21-SEP: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their September 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2021-36952 - Visual Studio Remote Code Execution Vulnerability
CVE-2021-36954 - Windows Bind Filter Driver Elevation of Privilege Vulnerability
CVE-2021-36955 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-36959 - Windows Authenticode Spoofing Vulnerability
CVE-2021-36960 - Windows SMB Information Disclosure Vulnerability
CVE-2021-36961 - Windows Installer Denial of Service Vulnerability
CVE-2021-36962 - Windows Installer Information Disclosure Vulnerability
CVE-2021-36963 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-36964 - Windows Event Tracing Elevation of Privilege Vulnerability

CVE-2021-36965 - Windows WLAN AutoConfig Service Remote Code Execution Vulnerability
CVE-2021-36966 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2021-36967 - Windows WLAN AutoConfig Service Elevation of Privilege Vulnerability
CVE-2021-36968 - Windows DNS Elevation of Privilege Vulnerability
CVE-2021-36969 - Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability
CVE-2021-36972 - Windows SMB Information Disclosure Vulnerability
CVE-2021-36973 - Windows Redirected Drive Buffering System Elevation of Privilege Vulnerability
CVE-2021-36974 - Windows SMB Elevation of Privilege Vulnerability
CVE-2021-36975 - Win32k Elevation of Privilege Vulnerability
CVE-2021-26435 - Windows Scripting Engine Memory Corruption Vulnerability
CVE-2021-26436 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2021-38624 - Windows Key Storage Provider Security Feature Bypass Vulnerability
CVE-2021-38625 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-38626 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2021-38628 - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2021-38629 - Windows Ancillary Function Driver for WinSock Information Disclosure Vulnerability
CVE-2021-38630 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2021-38632 - BitLocker Security Feature Bypass Vulnerability
CVE-2021-38633 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2021-38634 - Microsoft Windows Update Client Elevation of Privilege Vulnerability
CVE-2021-38635 - Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability
CVE-2021-38636 - Windows Redirected Drive Buffering SubSystem Driver Information Disclosure Vulnerability
CVE-2021-38637 - Windows Storage Information Disclosure Vulnerability
CVE-2021-38638 - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2021-38641 - Microsoft Edge for Android Spoofing Vulnerability
CVE-2021-38642 - Microsoft Edge for iOS Spoofing Vulnerability
CVE-2021-38645 - Open Management Infrastructure Elevation of Privilege Vulnerability
CVE-2021-38647 - Open Management Infrastructure Remote Code Execution Vulnerability
CVE-2021-38648 - Open Management Infrastructure Elevation of Privilege Vulnerability
CVE-2021-38649 - Open Management Infrastructure Elevation of Privilege Vulnerability
CVE-2021-38669 - Microsoft Edge (Chromium-based) Tampering Vulnerability
CVE-2021-26437 - Visual Studio Code Spoofing Vulnerability
CVE-2021-26439 - Microsoft Edge for Android Information Disclosure Vulnerability
CVE-2021-40440 - Microsoft Dynamics Business Central Cross-site Scripting Vulnerability
CVE-2021-36930 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2021-36956 - Azure Sphere Information Disclosure Vulnerability
CVE-2021-26434 - Visual Studio Elevation of Privilege Vulnerability
CVE-2021-38639 - Win32k Elevation of Privilege Vulnerability
CVE-2021-38644 - Microsoft MPEG-2 Video Extension Remote Code Execution Vulnerability
CVE-2021-38656 - Microsoft Word Remote Code Execution Vulnerability
CVE-2021-38657 - Microsoft Office Graphics Component Information Disclosure Vulnerability
CVE-2021-38659 - Microsoft Office Remote Code Execution Vulnerability
CVE-2021-38661 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2021-38667 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-38671 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-30606 - Chromium: CVE-2021-30606 Use after free in Blink

CVE-2021-30607 - Chromium: CVE-2021-30607 Use after free in Permissions
CVE-2021-30608 - Chromium: CVE-2021-30608 Use after free in Web Share
CVE-2021-30609 - Chromium: CVE-2021-30609 Use after free in Sign-In
CVE-2021-30610 - Chromium: CVE-2021-30610 Use after free in Extensions API
CVE-2021-30611 - Chromium: CVE-2021-30611 Use after free in WebRTC
CVE-2021-30612 - Chromium: CVE-2021-30612 Use after free in WebRTC
CVE-2021-30613 - Chromium: CVE-2021-30613 Use after free in Base internals
CVE-2021-30614 - Chromium: CVE-2021-30614 Heap buffer overflow in TabStrip
CVE-2021-30615 - Chromium: CVE-2021-30615 Cross-origin data leak in Navigation
CVE-2021-30616 - Chromium: CVE-2021-30616 Use after free in Media
CVE-2021-30617 - Chromium: CVE-2021-30617 Policy bypass in Blink
CVE-2021-30618 - Chromium: CVE-2021-30618 Inappropriate implementation in DevTools
CVE-2021-30619 - Chromium: CVE-2021-30619 UI Spoofing in Autofill
CVE-2021-30620 - Chromium: CVE-2021-30620 Insufficient policy enforcement in Blink
CVE-2021-30621 - Chromium: CVE-2021-30621 UI Spoofing in Autofill
CVE-2021-30622 - Chromium: CVE-2021-30622 Use after free in WebApp Installs
CVE-2021-30623 - Chromium: CVE-2021-30623 Use after free in Bookmarks
CVE-2021-30624 - Chromium: CVE-2021-30624 Use after free in Autofill
CVE-2021-40447 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2021-40448 - Microsoft Accessibility Insights for Android Information Disclosure Vulnerability
CVE-2021-30632 - Chromium: CVE-2021-30632 Out of bounds write in V8

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Microsoft Visual Studio 2019 version 16.4 (includes 16.0 - 16.3)
HEVC Video Extensions
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Azure Open Management Infrastructure
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Microsoft 365 Apps for Enterprise for 64-bit Systems
Windows Server 2022 (Server Core installation)
Windows Server 2019
Windows 8.1 for x64-based systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Microsoft Edge for Android
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 2004 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)

Windows 10 Version 2004 for ARM64-based Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server, version 2004 (Server Core installation)
Azure Sphere
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 â€“ 16.6)
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Microsoft Edge (Chromium-based)
Microsoft 365 Apps for Enterprise for 32-bit Systems
Windows Server 2022
Windows Server 2012
Accessibility Insights for Android
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Microsoft Dynamics 365 Business Central 2020 Release Wave 2 â€“ Update 17.10
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows 10 Version 1909 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
MPEG-2 Video Extension
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 2004 for 32-bit Systems
Windows Server 2019 (Server Core installation)
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft Dynamics 365 Business Central 2021 Release Wave 1 - Update 18.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30608
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36930
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30607

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30615
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30622
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30619
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30613
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30623
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30609
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26436
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38642
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30618
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30606
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30621
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30617
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38641
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30624
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30614
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30620
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30612
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30611
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26439
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30616
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30610
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38629
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38638
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38628

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38636
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38633
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40447
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36956
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38648
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38630
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38661
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36961
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40448
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38667
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36967
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36960
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26435
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38657
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36962
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38671
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36975
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26434
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36964
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36955
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36974
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-26437
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36965
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40440

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38645
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36963
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38624
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36968
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36959
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36972
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36969
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36954
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36973
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38649
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38669
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38656
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38635
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38639
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38647
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38659
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38637
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38632
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36966
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38626
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38625
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36952
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38644
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-38634

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30632
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38629
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36969
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30612
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36972
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30611
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38649
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38669
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26439
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38656
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38635
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30620
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36974
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36959
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30614
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38639

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30616
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38647
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36966
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30610
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38626
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38634
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38644
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30632
URL	https://support.microsoft.com/en-us/help/5005606
URL	https://support.microsoft.com/en-us/help/5005627
URL	https://support.microsoft.com/en-us/help/5005573
URL	https://support.microsoft.com/en-us/help/5005566
URL	https://support.microsoft.com/en-us/help/5005623
URL	https://support.microsoft.com/en-us/help/5005613
URL	https://support.microsoft.com/en-us/help/5005633
URL	https://support.microsoft.com/en-us/help/5005568
URL	https://support.microsoft.com/en-us/help/5005565
URL	https://support.microsoft.com/en-us/help/5005569
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30608

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38636
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36930
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40447
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36956
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38648
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38630
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30607
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38661
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40448
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38667
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30615
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38657
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26435
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36960
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36962
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38671

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30622
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26434
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26437
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36965
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-40440
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30619
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30613
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36963
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38624
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30623
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30609
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26436
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36968
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36954
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38642
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30618

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38659
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38637
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38632
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38625
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36952
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30606
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30621
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38638
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38628
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38633
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36961
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36967
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30617
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38641
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36975
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36964

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36955
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-30624
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38645
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36973
URL	https://support.microsoft.com/en-us/help/5006075
URL	https://support.microsoft.com/en-us/help/5005618
URL	https://support.microsoft.com/en-us/help/5006076
URL	https://support.microsoft.com/en-us/help/5005607
URL	https://support.microsoft.com/en-us/help/5005615

MS22-APR: Microsoft Windows Security Update

High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2022-22008 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2022-22009 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2022-21983 - Win32 Stream Enumeration Remote Code Execution Vulnerability
CVE-2022-23257 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2022-23268 - Windows Hyper-V Denial of Service Vulnerability
CVE-2022-23292 - Microsoft Power BI Spoofing Vulnerability
CVE-2022-24513 - Visual Studio Elevation of Privilege Vulnerability
CVE-2022-24521 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-24474 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2022-24523 - Microsoft Edge (Chromium-based) Spoofing Vulnerability
CVE-2022-24475 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-24484 - Windows Cluster Shared Volume (CSV) Denial of Service Vulnerability
CVE-2022-24533 - Remote Desktop Protocol Remote Code Execution Vulnerability
CVE-2022-24485 - Win32 File Enumeration Remote Code Execution Vulnerability
CVE-2022-24534 - Win32 Stream Enumeration Remote Code Execution Vulnerability
CVE-2022-24486 - Windows Kerberos Elevation of Privilege Vulnerability
CVE-2022-24544 - Windows Kerberos Elevation of Privilege Vulnerability
CVE-2022-24496 - Local Security Authority (LSA) Elevation of Privilege Vulnerability

CVE-2022-24545 - Windows Kerberos Remote Code Execution Vulnerability
CVE-2022-24548 - Microsoft Defender Denial of Service Vulnerability
CVE-2022-24549 - Windows AppX Package Manager Elevation of Privilege Vulnerability
CVE-2022-24500 - Windows SMB Remote Code Execution Vulnerability
CVE-2022-24550 - Windows Telephony Server Elevation of Privilege Vulnerability
CVE-2022-26786 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26787 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26788 - PowerShell Elevation of Privilege Vulnerability
CVE-2022-26789 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26790 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26791 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26792 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26793 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26794 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26795 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26796 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26797 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26798 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26811 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26812 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26813 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26891 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-26894 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-26895 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-26896 - Azure Site Recovery Information Disclosure Vulnerability
CVE-2022-26897 - Azure Site Recovery Information Disclosure Vulnerability
CVE-2022-26898 - Azure Site Recovery Remote Code Execution Vulnerability
CVE-2022-26900 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-26904 - Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2022-26914 - Win32k Elevation of Privilege Vulnerability
CVE-2022-26915 - Windows Secure Channel Denial of Service Vulnerability
CVE-2022-26916 - Windows Fax Compose Form Remote Code Execution Vulnerability
CVE-2022-26917 - Windows Fax Compose Form Remote Code Execution Vulnerability
CVE-2022-26918 - Windows Fax Compose Form Remote Code Execution Vulnerability
CVE-2022-26919 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-26920 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2022-23259 - Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability
CVE-2022-24527 - Windows Endpoint Configuration Manager Elevation of Privilege Vulnerability
CVE-2022-24479 - Connected User Experiences and Telemetry Elevation of Privilege Vulnerability
CVE-2022-24528 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2022-24481 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-24530 - Windows Installer Elevation of Privilege Vulnerability
CVE-2022-24482 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2022-24532 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-24483 - Windows Kernel Information Disclosure Vulnerability
CVE-2022-24487 - Windows Local Security Authority (LSA) Remote Code Execution Vulnerability
CVE-2022-24536 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-24488 - Windows Desktop Bridge Elevation of Privilege Vulnerability
CVE-2022-24537 - Windows Hyper-V Remote Code Execution Vulnerability

CVE-2022-24489 - Cluster Client Failover (CCF) Elevation of Privilege Vulnerability
CVE-2022-24538 - Windows Cluster Shared Volume (CSV) Denial of Service Vulnerability
CVE-2022-24490 - Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability
CVE-2022-24539 - Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability
CVE-2022-24491 - Windows Network File System Remote Code Execution Vulnerability
CVE-2022-24540 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2022-24492 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2022-24541 - Windows Server Service Remote Code Execution Vulnerability
CVE-2022-24493 - Microsoft Local Security Authority (LSA) Server Information Disclosure Vulnerability
CVE-2022-24542 - Windows Win32k Elevation of Privilege Vulnerability
CVE-2022-24494 - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2022-24543 - Windows Upgrade Assistant Remote Code Execution Vulnerability
CVE-2022-24495 - Windows Direct Show - Remote Code Execution Vulnerability
CVE-2022-24497 - Windows Network File System Remote Code Execution Vulnerability
CVE-2022-24546 - Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-24498 - Windows iSCSI Target Service Information Disclosure Vulnerability
CVE-2022-24547 - Windows Digital Media Receiver Elevation of Privilege Vulnerability
CVE-2022-24499 - Windows Installer Elevation of Privilege Vulnerability
CVE-2022-26783 - Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability
CVE-2022-26784 - Windows Cluster Shared Volume (CSV) Denial of Service Vulnerability
CVE-2022-26785 - Windows Hyper-V Shared Virtual Hard Disks Information Disclosure Vulnerability
CVE-2022-26801 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26802 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26803 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-26807 - Windows Work Folder Service Elevation of Privilege Vulnerability
CVE-2022-26808 - Windows File Explorer Elevation of Privilege Vulnerability
CVE-2022-26809 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2022-26810 - Windows File Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2022-26814 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26815 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26816 - Windows DNS Server Information Disclosure Vulnerability
CVE-2022-26817 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26818 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26819 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26820 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26821 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26822 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26823 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26824 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26825 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26826 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26827 - Windows File Server Resource Management Service Elevation of Privilege Vulnerability
CVE-2022-26828 - Windows Bluetooth Driver Elevation of Privilege Vulnerability
CVE-2022-26829 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-26830 - DiskUsage.exe Remote Code Execution Vulnerability
CVE-2022-26831 - Windows LDAP Denial of Service Vulnerability
CVE-2022-24765 - GitHub: Uncontrolled search for the Git directory in Git for Windows

CVE-2022-26907 - Azure SDK for .NET Information Disclosure Vulnerability
CVE-2022-26908 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-26909 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-24767 - GitHub: Git for Windows' uninstaller vulnerable to DLL hijacking when run under the SYSTEM user account
CVE-2022-26912 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-26921 - Visual Studio Code Elevation of Privilege Vulnerability
CVE-2022-26924 - YARP Denial of Service Vulnerability
CVE-2022-1125 - Chromium: CVE-2022-1125 Use after free in Portals
CVE-2022-1127 - Chromium: CVE-2022-1127 Use after free in QR Code Generator
CVE-2022-1128 - Chromium: CVE-2022-1128 Inappropriate implementation in Web Share API
CVE-2022-1129 - Chromium: CVE-2022-1129 Inappropriate implementation in Full Screen Mode
CVE-2022-1130 - Chromium: CVE-2022-1130 Insufficient validation of untrusted input in WebOTP
CVE-2022-1131 - Chromium: CVE-2022-1131 Use after free in Cast UI
CVE-2022-1133 - Chromium: CVE-2022-1133 Use after free in WebRTC
CVE-2022-1134 - Chromium: CVE-2022-1134 Type Confusion in V8
CVE-2022-1135 - Chromium: CVE-2022-1135 Use after free in Shopping Cart
CVE-2022-1136 - Chromium: CVE-2022-1136 Use after free in Tab Strip
CVE-2022-1137 - Chromium: CVE-2022-1137 Inappropriate implementation in Extensions
CVE-2022-1138 - Chromium: CVE-2022-1138 Inappropriate implementation in Web Cursor
CVE-2022-1143 - Chromium: CVE-2022-1143 Heap buffer overflow in WebUI
CVE-2022-1145 - Chromium: CVE-2022-1145 Use after free in Extensions
CVE-2022-1146 - Chromium: CVE-2022-1146 Inappropriate implementation in Resource Timing
CVE-2022-1139 - Chromium: CVE-2022-1139 Inappropriate implementation in Background Fetch API
CVE-2022-1232 - Chromium: CVE-2022-1232 Type Confusion in V8

Affected Products:
HEVC Video Extensions
Windows 11 for ARM64-based Systems
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Azure SDK for .Net
Windows Server 2019 (Server Core installation)
Windows 10 Version 21H2 for 32-bit Systems
Microsoft On-Premises Data Gateway
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
YARP 1.1RC
Microsoft Malware Protection Engine
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1909 for x64-based Systems
Windows 8.1 for 32-bit systems
HEVC Video Extension
Windows 10 Version 1607 for 32-bit Systems
Windows Server 2022 (Server Core installation)
Windows 10 Version 21H2 for x64-based Systems
Windows 7 for x64-based Systems Service Pack 1
Microsoft Visual Studio 2022 version 17.1
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 1607 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)

Windows RT 8.1
Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 21H1 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 for x64-based Systems
Windows Server 2012 (Server Core installation)
Windows Server 2012 R2
Windows Server 2016
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 1909 for 32-bit Systems
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 �" 16.6)
Microsoft Visual Studio 2022 version 17.0
Azure Site Recovery VMWare to Azure
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 11 for x64-based Systems
Microsoft Edge (Chromium-based)
Visual Studio 2019 for Mac version 8.10
Windows Upgrade Assistant
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 1809 for 32-bit Systems
Visual Studio Code
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2022
Windows Server 2012
YARP 1.0
Windows Server 2019
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 for 32-bit Systems
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows 8.1 for x64-based systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Dynamics 365 (on-premises) version 9.1
Windows 10 Version 1909 for ARM64-based Systems

Solution Details

Microsoft has released a fix for this flaw in their April 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24533
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24534
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21983
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24492
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24539
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26921
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24513
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26811
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26809
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26822
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26783
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26814
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23292
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26897
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24483
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26819
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26801
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23259
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26792
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26924
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24482
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24547
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26793

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24493
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26823
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24521
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24765
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24541
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24498
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26918
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26820
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24485
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24490
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26796
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26828
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24496
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26916
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26785
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22009
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26790
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24544
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24549
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26798
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24527
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26826
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26825
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26830

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24488
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24500
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26786
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24495
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26915
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23257
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26817
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26795
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26807
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24486
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26788
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24537
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24474
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24484
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26813
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24479
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24489
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26898
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24545
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26831
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24481
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26784
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26803
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26896

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26789
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24494
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26914
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26791
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24532
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26919
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24499
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24546
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26829
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26802
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26824
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24550
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24540
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22008
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26812
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26821
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26794
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24491
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24548
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26904
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26907
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24528
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26797
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24543

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26827
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26815
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24497
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26917
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26816
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23268
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24538
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26787
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24530
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26808
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24536
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24767
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26818
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26920
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26810
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24542
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24487
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1232
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1125
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1131
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1135
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1136
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1137
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1127

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1138
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1128
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1133
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1134
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1129
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1139
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1146
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1143
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-1130
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26891
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24523
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24475
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26912
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26908
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26900
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26894
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26909
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26895
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26794
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1135
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24491

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24479
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26813
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24489
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24474
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24484
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26898
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26831
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24533
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24545
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26789
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24481
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26784
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26803
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26896
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24538
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26787

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26816
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23268
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1128
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1127
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24530
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26808
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24767
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26818
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26920
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24536
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24487
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1133
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26810
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24542
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24528
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26797

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26907
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1129
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24543
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26827
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24497
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26917
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26815
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24547
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24482
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26793
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24493
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26823
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1137
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1138
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24521
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24539

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26921
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24534
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24492
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21983
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1143
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26822
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26783
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24513
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26811
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26809
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24483
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26897
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26801
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26819
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23259
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26814

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23292
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26924
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26792
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1139
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26825
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26830
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24488
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1131
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1125
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23257
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26817
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24500
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26786
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24495
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26915
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26807

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26795
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24486
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26788
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1130
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24537
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26918
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24498
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1145
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26820
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1232
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24765
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24541
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24485
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24490
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26796
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26828

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26916
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24496
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1146
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22009
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26785
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26790
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24549
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26798
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26826
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24527
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24544
URL	https://support.microsoft.com/en-us/help/5012632
URL	https://support.microsoft.com/en-us/help/5012592
URL	https://support.microsoft.com/en-us/help/5012626
URL	https://support.microsoft.com/en-us/help/5012599
URL	https://support.microsoft.com/en-us/help/5012604
URL	https://support.microsoft.com/en-us/help/5012666
URL	https://support.microsoft.com/en-us/help/5012653
URL	https://support.microsoft.com/en-us/help/5012647

Type	Reference
URL	https://support.microsoft.com/en-us/help/5012658
URL	https://support.microsoft.com/en-us/help/5012732
URL	https://support.microsoft.com/en-us/help/5012596
URL	https://support.microsoft.com/en-us/help/5012639
URL	https://support.microsoft.com/en-us/help/5012591
URL	https://support.microsoft.com/en-us/help/5012731
URL	https://support.microsoft.com/en-us/help/5012650
URL	https://support.microsoft.com/en-us/help/5012649
URL	https://support.microsoft.com/en-us/help/5012670
URL	https://github.com/git-for-windows/git/security/advisories/GHSA-vw2c-22j4-2fh2
URL	https://github.com/git-for-windows/git/security/advisories/GHSA-gf48-x3vr-j5c3
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26891
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24523
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24475
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26912
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26908
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26900
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26894
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26909

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26895
URL	https://support.microsoft.com/en-us/help/5011529
URL	https://support.microsoft.com/en-us/help/5011552
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26919
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24499
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1134
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26914
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24494
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26791
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24532
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26802
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-1136
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26824
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24550
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24546
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26829

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26821
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24540
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22008
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26812
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24548
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26904

MS22-FEB: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their February 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2022-21971 - Windows Runtime Remote Code Execution Vulnerability
CVE-2022-21981 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-21974 - Roaming Security Rights Management Services Remote Code Execution Vulnerability
CVE-2022-21844 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-21926 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-21927 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-21957 - Microsoft Dynamics 365 (on-premises) Remote Code Execution Vulnerability
CVE-2022-21965 - Microsoft Teams Denial of Service Vulnerability
CVE-2022-22709 - VP9 Video Extensions Remote Code Execution Vulnerability
CVE-2022-22710 - Windows Common Log File System Driver Denial of Service Vulnerability
CVE-2022-22712 - Windows Hyper-V Denial of Service Vulnerability
CVE-2022-23254 - Microsoft Power BI Information Disclosure Vulnerability
CVE-2022-23269 - Microsoft Dynamics GP Spoofing Vulnerability
CVE-2022-23271 - Microsoft Dynamics GP Elevation Of Privilege Vulnerability
CVE-2022-23272 - Microsoft Dynamics GP Elevation Of Privilege Vulnerability
CVE-2022-23273 - Microsoft Dynamics GP Elevation Of Privilege Vulnerability
CVE-2022-23274 - Microsoft Dynamics GP Remote Code Execution Vulnerability

CVE-2022-22715 - Named Pipe File System Elevation of Privilege Vulnerability
CVE-2022-22717 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-22718 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-21984 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-21985 - Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2022-21986 - .NET Denial of Service Vulnerability
CVE-2022-21989 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-21991 - Visual Studio Code Remote Development Extension Remote Code Execution Vulnerability
CVE-2022-21992 - Windows Mobile Device Management Remote Code Execution Vulnerability
CVE-2022-21993 - Windows Services for NFS ONCRPC XDR Driver Information Disclosure Vulnerability
CVE-2022-21994 - Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-21995 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2022-21996 - Win32k Elevation of Privilege Vulnerability
CVE-2022-21997 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-21998 - Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2022-21999 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-22000 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-22001 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2022-22002 - Windows User Account Profile Picture Denial of Service Vulnerability
CVE-2022-23255 - Microsoft OneDrive for Android Security Feature Bypass Vulnerability
CVE-2022-23261 - Microsoft Edge (Chromium-based) Tampering Vulnerability
CVE-2022-23262 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-23263 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-0452 - Chromium: CVE-2022-0452 Use after free in Safe Browsing
CVE-2022-0453 - Chromium: CVE-2022-0453 Use after free in Reader Mode
CVE-2022-0454 - Chromium: CVE-2022-0454 Heap buffer overflow in ANGLE
CVE-2022-0455 - Chromium: CVE-2022-0455 Inappropriate implementation in Full Screen Mode
CVE-2022-0456 - Chromium: CVE-2022-0456 Use after free in Web Search
CVE-2022-0457 - Chromium: CVE-2022-0457 Type Confusion in V8
CVE-2022-0458 - Chromium: CVE-2022-0458 Use after free in Thumbnail Tab Strip
CVE-2022-0459 - Chromium: CVE-2022-0459 Use after free in Screen Capture
CVE-2022-0460 - Chromium: CVE-2022-0460 Use after free in Window Dialog
CVE-2022-0461 - Chromium: CVE-2022-0461 Policy bypass in COOP
CVE-2022-0462 - Chromium: CVE-2022-0462 Inappropriate implementation in Scroll
CVE-2022-0463 - Chromium: CVE-2022-0463 Use after free in Accessibility
CVE-2022-0464 - Chromium: CVE-2022-0464 Use after free in Accessibility
CVE-2022-0465 - Chromium: CVE-2022-0465 Use after free in Extensions
CVE-2022-0466 - Chromium: CVE-2022-0466 Inappropriate implementation in Extensions Platform
CVE-2022-0467 - Chromium: CVE-2022-0467 Inappropriate implementation in Pointer Lock
CVE-2022-0468 - Chromium: CVE-2022-0468 Use after free in Payments
CVE-2022-0469 - Chromium: CVE-2022-0469 Use after free in Cast
CVE-2022-0470 - Chromium: CVE-2022-0470 Out of bounds memory access in V8

Affected Products:
PowerBI-client JS SDK
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows Server, version 20H2 (Server Core Installation)

HEVC Video Extensions
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Microsoft Edge (Chromium-based)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 21H2 for x64-based Systems
Windows Server 2012 (Server Core installation)
Windows Server 2022 (Server Core installation)
Windows Server 2022
Microsoft Visual Studio 2022 version 17.0
Windows Server 2012
Windows Server 2019
Windows 7 for x64-based Systems Service Pack 1
Visual Studio Code
Microsoft Teams for iOS
.NET 5.0
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Teams Admin Center
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 10 Version 21H2 for ARM64-based Systems
Windows 8.1 for 32-bit systems
Visual Studio 2019 for Mac version 8.10
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 11 for x64-based Systems
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Windows 10 Version 1909 for ARM64-based Systems
Microsoft Dynamics 365 (on-premises) version 9.0
Microsoft Dynamics 365 (on-premises) version 8.2
HEVC Video Extension
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Windows 11 for ARM64-based Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
OneDrive for Android

VP9 Video Extensions
Microsoft Dynamics GP
Windows Server 2019 (Server Core installation)
Microsoft Teams for Android
Windows Server 2016
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server 2022 Azure Edition Core Hotpatch
.NET 6.0
Windows 10 Version 21H1 for ARM64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23272
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0464
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0460
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0465
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0459
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0461
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0463
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0458
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0462
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0456
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0453
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0457
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0452
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0469
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0466

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0454
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0467
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0470
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0468
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0455
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23263
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23262
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23261
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21965
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21992
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22002
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22717
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22715
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22712
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21998
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21986
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21844
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21996
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22710
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21985
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23254
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21994
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23274
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21926

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21995
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23271
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21927
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21991
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22001
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21989
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21997
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22000
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21971
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23269
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21981
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22709
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23255
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23273
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21984
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21974
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21999
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21957
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21993
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22718
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23263
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23262
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23261

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21992
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21965
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0464
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0460
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22002
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0465
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22717
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22715
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0459
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22712
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21998
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21986
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21844
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23272
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21996
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22710

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0463
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0461
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21985
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0458
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0462
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23254
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0456
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21994
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0453
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23274
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0457
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21926
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21995
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0452
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23271
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21927

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21991
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22001
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21989
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21997
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22000
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21971
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23269
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21981
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0469
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22709
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0466
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23255
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23273
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21984
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21999
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21957

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21974
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21993
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0454
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0467
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0470
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0468
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0455
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22718
URL	https://support.microsoft.com/en-us/help/5010351
URL	https://support.microsoft.com/en-us/help/5010354
URL	https://support.microsoft.com/en-us/help/5010342
URL	https://support.microsoft.com/en-us/help/5010395
URL	https://support.microsoft.com/en-us/help/5010412
URL	https://support.microsoft.com/en-us/help/5010422
URL	https://support.microsoft.com/en-us/help/5010419
URL	https://support.microsoft.com/en-us/help/5010403
URL	https://support.microsoft.com/en-us/help/5010345
URL	https://support.microsoft.com/en-us/help/5010358
URL	https://support.microsoft.com/en-us/help/5010384
URL	https://support.microsoft.com/en-us/help/5010404

Type	Reference
URL	https://support.microsoft.com/en-us/help/5010386
URL	https://support.microsoft.com/en-us/help/5010359
URL	https://support.microsoft.com/en-us/help/5010392
URL	https://support.microsoft.com/en-us/help/5010456

MS22-JAN: Microsoft Windows Security Update High

Solution Details

Microsoft has released a fix for this flaw in their January 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2022-21852 - Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2021-22947 - Open Source Curl Remote Code Execution Vulnerability
CVE-2021-36976 - Libarchive Remote Code Execution Vulnerability
CVE-2022-21919 - Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2022-21918 - DirectX Graphics Kernel File Denial of Service Vulnerability
CVE-2022-21917 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-21915 - Windows GDI+ Information Disclosure Vulnerability
CVE-2022-21932 - Microsoft Dynamics 365 Customer Engagement Cross-Site Scripting Vulnerability
CVE-2022-21833 - Virtual Machine IDE Drive Elevation of Privilege Vulnerability
CVE-2022-21834 - Windows User-mode Driver Framework Reflector Driver Elevation of Privilege Vulnerability
CVE-2022-21835 - Microsoft Cryptographic Services Elevation of Privilege Vulnerability
CVE-2022-21836 - Windows Certificate Spoofing Vulnerability
CVE-2022-21838 - Windows Cleanup Manager Elevation of Privilege Vulnerability
CVE-2022-21839 - Windows Event Tracing Discretionary Access Control List Denial of Service Vulnerability
CVE-2022-21857 - Active Directory Domain Services Elevation of Privilege Vulnerability
CVE-2022-21858 - Windows Bind Filter Driver Elevation of Privilege Vulnerability
CVE-2022-21859 - Windows Accounts Control Elevation of Privilege Vulnerability
CVE-2022-21860 - Windows AppContracts API Server Elevation of Privilege Vulnerability
CVE-2022-21861 - Task Flow Data Engine Elevation of Privilege Vulnerability
CVE-2022-21862 - Windows Application Model Core API Elevation of Privilege Vulnerability
CVE-2022-21863 - Windows StateRepository API Server file Elevation of Privilege Vulnerability

CVE-2022-21864 - Windows UI Immersive Server API Elevation of Privilege Vulnerability
CVE-2022-21865 - Connected Devices Platform Service Elevation of Privilege Vulnerability
CVE-2022-21866 - Windows System Launcher Elevation of Privilege Vulnerability
CVE-2022-21867 - Windows Push Notifications Apps Elevation Of Privilege Vulnerability
CVE-2022-21868 - Windows Devices Human Interface Elevation of Privilege Vulnerability
CVE-2022-21869 - Clipboard User Service Elevation of Privilege Vulnerability
CVE-2022-21870 - Tablet Windows User Interface Application Core Elevation of Privilege Vulnerability
CVE-2022-21871 - Microsoft Diagnostics Hub Standard Collector Runtime Elevation of Privilege Vulnerability
CVE-2022-21872 - Windows Event Tracing Elevation of Privilege Vulnerability
CVE-2022-21873 - Tile Data Repository Elevation of Privilege Vulnerability
CVE-2022-21874 - Windows Security Center API Remote Code Execution Vulnerability
CVE-2022-21875 - Windows Storage Elevation of Privilege Vulnerability
CVE-2022-21876 - Win32k Information Disclosure Vulnerability
CVE-2022-21877 - Storage Spaces Controller Information Disclosure Vulnerability
CVE-2022-21878 - Windows Geolocation Service Remote Code Execution Vulnerability
CVE-2022-21879 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-21880 - Windows GDI+ Information Disclosure Vulnerability
CVE-2022-21881 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-21882 - Win32k Elevation of Privilege Vulnerability
CVE-2022-21843 - Windows IKE Extension Denial of Service Vulnerability
CVE-2022-21883 - Windows IKE Extension Denial of Service Vulnerability
CVE-2022-21884 - Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
CVE-2022-21885 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2022-21887 - Win32k Elevation of Privilege Vulnerability
CVE-2022-21888 - Windows Modern Execution Server Remote Code Execution Vulnerability
CVE-2022-21892 - Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21893 - Remote Desktop Protocol Remote Code Execution Vulnerability
CVE-2022-21894 - Secure Boot Security Feature Bypass Vulnerability
CVE-2022-21900 - Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2022-21901 - Windows Hyper-V Elevation of Privilege Vulnerability
CVE-2022-21902 - Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-21903 - Windows GDI Elevation of Privilege Vulnerability
CVE-2022-21904 - Windows GDI Information Disclosure Vulnerability
CVE-2022-21905 - Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2022-21906 - Windows Defender Application Control Security Feature Bypass Vulnerability
CVE-2022-21907 - HTTP Protocol Stack Remote Code Execution Vulnerability
CVE-2022-21908 - Windows Installer Elevation of Privilege Vulnerability
CVE-2022-21910 - Microsoft Cluster Port Driver Elevation of Privilege Vulnerability
CVE-2022-21912 - DirectX Graphics Kernel Remote Code Execution Vulnerability
CVE-2022-21913 - Local Security Authority (Domain Policy) Remote Protocol Security Feature Bypass
CVE-2022-21924 - Workstation Service Remote Protocol Security Feature Bypass Vulnerability
CVE-2022-21925 - Windows BackupKey Remote Protocol Security Feature Bypass Vulnerability
CVE-2022-21958 - Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21959 - Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21960 - Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21961 - Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21962 - Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21963 - Windows Resilient File System (ReFS) Remote Code Execution Vulnerability

CVE-2022-21964 - Remote Desktop Licensing Diagnoser Information Disclosure Vulnerability
CVE-2022-21847 - Windows Hyper-V Denial of Service Vulnerability
CVE-2022-21922 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2022-21921 - Windows Defender Credential Guard Security Feature Bypass Vulnerability
CVE-2022-21920 - Windows Kerberos Elevation of Privilege Vulnerability
CVE-2022-21848 - Windows IKE Extension Denial of Service Vulnerability
CVE-2022-21849 - Windows IKE Extension Remote Code Execution Vulnerability
CVE-2022-21850 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2022-21851 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2022-21916 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-21895 - Windows User Profile Service Elevation of Privilege Vulnerability
CVE-2022-21914 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2022-21889 - Windows IKE Extension Denial of Service Vulnerability
CVE-2022-21890 - Windows IKE Extension Denial of Service Vulnerability
CVE-2022-21891 - Microsoft Dynamics 365 (on-premises) Spoofing Vulnerability
CVE-2022-21896 - Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-21897 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-21898 - DirectX Graphics Kernel Remote Code Execution Vulnerability
CVE-2022-21899 - Windows Extensible Firmware Interface Security Feature Bypass Vulnerability
CVE-2022-21928 - Windows Resilient File System (ReFS) Remote Code Execution Vulnerability
CVE-2022-21929 - Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2022-21930 - Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2022-21931 - Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2022-21954 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-21970 - Microsoft Edge (Chromium-based) Elevation of Privilege Vulnerability
CVE-2022-0096 - Chromium: CVE-2022-0096 Use after free in Storage
CVE-2022-0097 - Chromium: CVE-2022-0097 Inappropriate implementation in DevTools
CVE-2022-0098 - Chromium: CVE-2022-0098 Use after free in Screen Capture
CVE-2022-0099 - Chromium: CVE-2022-0099 Use after free in Sign-in
CVE-2022-0100 - Chromium: CVE-2022-0100 Heap buffer overflow in Media streams API
CVE-2022-0101 - Chromium: CVE-2022-0101 Heap buffer overflow in Bookmarks
CVE-2022-0102 - Chromium: CVE-2022-0102 Type Confusion in V8
CVE-2022-0103 - Chromium: CVE-2022-0103 Use after free in SwiftShader
CVE-2022-0104 - Chromium: CVE-2022-0104 Heap buffer overflow in ANGLE
CVE-2022-0105 - Chromium: CVE-2022-0105 Use after free in PDF
CVE-2022-0106 - Chromium: CVE-2022-0106 Use after free in Autofill
CVE-2022-0107 - Chromium: CVE-2022-0107 Use after free in File Manager API
CVE-2022-0108 - Chromium: CVE-2022-0108 Inappropriate implementation in Navigation
CVE-2022-0109 - Chromium: CVE-2022-0109 Inappropriate implementation in Autofill
CVE-2022-0110 - Chromium: CVE-2022-0110 Incorrect security UI in Autofill
CVE-2022-0111 - Chromium: CVE-2022-0111 Inappropriate implementation in Navigation
CVE-2022-0112 - Chromium: CVE-2022-0112 Incorrect security UI in Browser UI
CVE-2022-0113 - Chromium: CVE-2022-0113 Inappropriate implementation in Blink
CVE-2022-0114 - Chromium: CVE-2022-0114 Out of bounds memory access in Web Serial
CVE-2022-0115 - Chromium: CVE-2022-0115 Uninitialized Use in File API
CVE-2022-0116 - Chromium: CVE-2022-0116 Inappropriate implementation in Compositing
CVE-2022-0117 - Chromium: CVE-2022-0117 Policy bypass in Service Workers
CVE-2022-0118 - Chromium: CVE-2022-0118 Inappropriate implementation in WebShare
CVE-2022-0120 - Chromium: CVE-2022-0120 Inappropriate implementation in Passwords

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
HEVC Video Extensions
Windows 10 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 21H1 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Windows Server 2022 (Server Core installation)
Windows Server 2019
Windows 8.1 for x64-based systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows 11 for x64-based Systems
Dynamics 365 Sales
Windows 10 Version 1607 for x64-based Systems
Windows Server 2016 (Server Core installation)
Windows 10 Version 1809 for 32-bit Systems
Remote Desktop client for Windows Desktop
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 10 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Dynamics 365 Customer Engagement V9.1
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows Server, version 20H2 (Server Core Installation)
Microsoft Edge (Chromium-based)
Windows 10 Version 21H2 for x64-based Systems
Windows Server 2022
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows 11 for ARM64-based Systems
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1909 for 32-bit Systems
Windows Server 2019 (Server Core installation)

Windows Server 2016
Microsoft Dynamics 365 Customer Engagement V9.0
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21913
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21881
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21873
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21915
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21900
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21868
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21858
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21910
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21925
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21859
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21852
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21894
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21882
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21887
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21963
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21843
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21883
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21908
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21895
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21876
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21964

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21874
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21901
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21864
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21919
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21905
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21916
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21870
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21896
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21922
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21932
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21961
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21902
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21836
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21921
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21839
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21897
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21890
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21884
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21903
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21865
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21862
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21917
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21892
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21899

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21962
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21918
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36976
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22947
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21866
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21888
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21960
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21833
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21877
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21860
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21907
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21851
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21893
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21834
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21850
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21928
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21835
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21889
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21871
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21904
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21867
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21912
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21857
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21849

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21958
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21879
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21959
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21861
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21880
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21878
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21847
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21920
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21872
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21914
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21838
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21863
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21869
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21848
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21906
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21885
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21898
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21924
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21891
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21875
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0113
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0107
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0097
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0100

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0098
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0108
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0118
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0102
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0109
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0106
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0099
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0096
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0117
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0105
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0110
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0104
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0112
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0103
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0120
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0114
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0116
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0115
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0111
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0101
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21970
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21929
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21930
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21931

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21954
URL	https://support.microsoft.com/en-us/help/5009610
URL	https://support.microsoft.com/en-us/help/5009619
URL	https://support.microsoft.com/en-us/help/5009601
URL	https://support.microsoft.com/en-us/help/5009555
URL	https://support.microsoft.com/en-us/help/5009566
URL	https://support.microsoft.com/en-us/help/5009557
URL	https://support.microsoft.com/en-us/help/5009627
URL	https://support.microsoft.com/en-us/help/5009595
URL	https://support.microsoft.com/en-us/help/5009621
URL	https://support.microsoft.com/en-us/help/5009624
URL	https://support.microsoft.com/en-us/help/5009545
URL	https://support.microsoft.com/en-us/help/5009543
URL	https://support.microsoft.com/en-us/help/5009546
URL	https://support.microsoft.com/en-us/help/5009586
URL	https://support.microsoft.com/en-us/help/5009585
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21924
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21891
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21931
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21906
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21885

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21898
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21869
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21848
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21838
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21863
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21872
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21914
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21880
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21878
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21847
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21920
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21861
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21959
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21879
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21958
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21857

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21849
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21912
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21867
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21904
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21871
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21929
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21889
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21835
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21928
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21850
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21834
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0100
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21893
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21851
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21907
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21860

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21877
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0111
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0115
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21833
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21970
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21960
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21888
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0114
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0103
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21866
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21913
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21881
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0104
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21873
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0110
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0099

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0106
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21915
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21900
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21868
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-22947
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0108
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21858
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0098
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21910
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21925
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21859
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21852
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0107
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0101
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21894
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21882

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21887
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0116
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21963
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0120
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21843
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21883
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21908
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21930
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0112
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0117
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21895
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21876
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0102
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36976
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21954
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21964

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0113
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21874
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21901
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21919
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21864
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21905
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21870
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21916
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21896
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21922
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0105
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21932
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21961
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0096
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21836
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21902

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21921
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21839
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0109
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21890
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21897
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0118
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21884
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21903
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21917
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21862
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21865
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21875
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21892
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21962
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0097
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21918

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21899

MS22-JUL: Microsoft Windows Security Update

High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2022-21845 - Windows Kernel Information Disclosure Vulnerability
CVE-2022-22711 - Windows BitLocker Information Disclosure Vulnerability
CVE-2022-30181 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33637 - Microsoft Defender for Endpoint Tampering Vulnerability
CVE-2022-33641 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33642 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33643 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-30187 - Azure Storage Library Information Disclosure Vulnerability
CVE-2022-30202 - Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability
CVE-2022-30203 - Windows Boot Manager Security Feature Bypass Vulnerability
CVE-2022-30205 - Windows Group Policy Elevation of Privilege Vulnerability
CVE-2022-30206 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-30208 - Windows Security Account Manager (SAM) Denial of Service Vulnerability
CVE-2022-30209 - Windows IIS Server Elevation of Privilege Vulnerability
CVE-2022-30211 - Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability
CVE-2022-30212 - Windows Connected Devices Platform Service Information Disclosure Vulnerability
CVE-2022-30213 - Windows GDI+ Information Disclosure Vulnerability
CVE-2022-30214 - Windows DNS Server Remote Code Execution Vulnerability
CVE-2022-30215 - Active Directory Federation Services Elevation of Privilege Vulnerability
CVE-2022-30216 - Windows Server Service Tampering Vulnerability
CVE-2022-30220 - Windows Common Log File System Driver Elevation of Privilege Vulnerability
CVE-2022-30221 - Windows Graphics Component Remote Code Execution Vulnerability
CVE-2022-30222 - Windows Shell Remote Code Execution Vulnerability
CVE-2022-30223 - Windows Hyper-V Information Disclosure Vulnerability
CVE-2022-30224 - Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability
CVE-2022-30225 - Windows Media Player Network Sharing Service Elevation of Privilege Vulnerability
CVE-2022-30226 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-22022 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-22023 - Windows Portable Device Enumerator Service Security Feature Bypass Vulnerability
CVE-2022-22024 - Windows Fax Service Remote Code Execution Vulnerability
CVE-2022-22025 - Windows Internet Information Services Cachuri Module Denial of Service Vulnerability
CVE-2022-22026 - Windows CSRSS Elevation of Privilege Vulnerability
CVE-2022-22027 - Windows Fax Service Remote Code Execution Vulnerability
CVE-2022-22028 - Windows Network File System Information Disclosure Vulnerability
CVE-2022-22029 - Windows Network File System Remote Code Execution Vulnerability
CVE-2022-22031 - Windows Credential Guard Domain-joined Public Key Elevation of Privilege

Vulnerability
CVE-2022-22034 - Windows Graphics Component Elevation of Privilege Vulnerability
CVE-2022-22036 - Performance Counters for Windows Elevation of Privilege Vulnerability
CVE-2022-22037 - Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability
CVE-2022-22038 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2022-22039 - Windows Network File System Remote Code Execution Vulnerability
CVE-2022-22040 - Internet Information Services Dynamic Compression Module Denial of Service Vulnerability
CVE-2022-22041 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-22042 - Windows Hyper-V Information Disclosure Vulnerability
CVE-2022-22043 - Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
CVE-2022-22045 - Windows.Devices.Picker.dll Elevation of Privilege Vulnerability
CVE-2022-22047 - Windows CSRSS Elevation of Privilege Vulnerability
CVE-2022-22048 - BitLocker Security Feature Bypass Vulnerability
CVE-2022-22049 - Windows CSRSS Elevation of Privilege Vulnerability
CVE-2022-22050 - Windows Fax Service Elevation of Privilege Vulnerability
CVE-2022-27776 - HackerOne: CVE-2022-27776 Insufficiently protected credentials vulnerability might leak authentication or cookie header data
CVE-2022-33644 - Xbox Live Save Service Elevation of Privilege Vulnerability
CVE-2022-33650 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-23816 - AMD: CVE-2022-23816 AMD CPU Branch Type Confusion
CVE-2022-33651 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33652 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33653 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33654 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33655 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33656 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33657 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33658 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33659 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33660 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33661 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33662 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33663 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33664 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33665 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33666 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33667 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33668 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33669 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33671 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33672 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-23825 - AMD: CVE-2022-23825 AMD CPU Branch Type Confusion
CVE-2022-33673 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33674 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33675 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33676 - Azure Site Recovery Remote Code Execution Vulnerability
CVE-2022-33677 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-33678 - Azure Site Recovery Remote Code Execution Vulnerability

CVE-2022-2294 - Chromium: CVE-2022-2294 Heap buffer overflow in WebRTC
CVE-2022-2295 - Chromium: CVE-2022-2295 Type Confusion in V8

Affected Products:
Windows Server 2012 (Server Core installation)
Windows 11 for ARM64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows Server 2016
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for x64-based Systems
Azure Storage Queues client library for .NET
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Azure Storage Queues client library for Python
Windows Server 2012 R2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 8.1 for x64-based systems
Microsoft Defender for Endpoint for Linux
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2019 (Server Core installation)
Windows 10 Version 21H2 for ARM64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2016 (Server Core installation)
Windows 10 Version 21H2 for x64-based Systems
Windows 11 for x64-based Systems
Windows 8.1 for 32-bit systems
Windows 10 Version 21H1 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows Server 2012
Windows Server, version 20H2 (Server Core Installation)
Azure Storage Blobs client library for Python
Windows Server 2019
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Edge (Chromium-based)
Windows Server 2022
Azure Storage Blobs client library for Java
Azure Storage Blobs client library for .NET
Windows 10 Version 21H2 for 32-bit Systems
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1809 for x64-based Systems
Remote Desktop client for Windows Desktop
Windows 10 for 32-bit Systems
Windows Server 2022 (Server Core installation)
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 20H2 for ARM64-based Systems

Windows Server 2012 R2
Azure Site Recovery VMWare to Azure
Windows 10 Version 20H2 for 32-bit Systems
Windows RT 8.1

Solution Details

Microsoft has released a fix for this flaw in their July 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2295
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2294
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22025
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-27776
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30202
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33656
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22026
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33644
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22038
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30215
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30213
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33650
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33674
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33659
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22029
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22047

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22041
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33672
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30221
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33642
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33668
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33663
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33665
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30181
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30187
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22034
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33651
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30214
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33678
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33675
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33673
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22027
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33643
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33657
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33662
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22049
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22040
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33637
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30208
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30205

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30203
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33664
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30226
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30212
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30220
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22042
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30224
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33666
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33669
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33660
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21845
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22050
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30216
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33641
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22036
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33677
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23816
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33655
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33653
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22023
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33658
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22028
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30222
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22039

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33671
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22711
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30209
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33661
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23825
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22022
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33652
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30206
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33667
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30225
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30223
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22048
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22043
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22045
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22031
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30211
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22024
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33654
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22037
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-33676
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22022
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33667
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30225

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30223
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22045
URL	https://support.microsoft.com/en-us/help/5015811
URL	https://support.microsoft.com/en-us/help/5015877
URL	https://support.microsoft.com/en-us/help/5015866
URL	https://support.microsoft.com/en-us/help/5015875
URL	https://support.microsoft.com/en-us/help/5015832
URL	https://support.microsoft.com/en-us/help/5015827
URL	https://support.microsoft.com/en-us/help/5015862
URL	https://support.microsoft.com/en-us/help/5015807
URL	https://support.microsoft.com/en-us/help/5015814
URL	https://support.microsoft.com/en-us/help/5015874
URL	https://support.microsoft.com/en-us/help/5015861
URL	https://support.microsoft.com/en-us/help/5015870
URL	https://support.microsoft.com/en-us/help/5015808
URL	https://support.microsoft.com/en-us/help/5015863
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30181
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30187
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33672
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30221
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33642

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33668
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33663
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33665
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22047
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2294
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22041
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22026
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33644
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33656
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30202
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30213
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22038
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30215
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33650
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33674
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22029

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33659
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30208
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30205
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30203
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33664
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30226
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30212
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30220
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22049
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33637
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22040
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22034
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33651
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30214
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33678
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33675

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33673
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33643
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22027
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33657
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33662
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33641
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30216
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22036
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33677
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23816
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22025
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33653
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33655
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22023
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22028
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33658

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22039
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33671
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30222
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21845
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22050
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-27776
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30224
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33666
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33669
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33660
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22042
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22031
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30211
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22024
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33654
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22037

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33676
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22048
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22043
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2295
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22711
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33661
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30209
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23825
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30206
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-33652

MS22-JUN: Microsoft SQL Server Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their June 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft SQL Server which include fixes for the following vulnerabilities:

CVE-2022-29143 - Microsoft SQL Server Remote Code Execution Vulnerability

Affected Products:
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (CU 17)
Microsoft SQL Server 2017 for x64-based Systems (GDR)

Microsoft SQL Server 2017 for x64-based Systems (CU 29)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)
Microsoft SQL Server 2019 for x64-based Systems (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 (GDR)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (GDR)
Microsoft SQL Server 2019 for x64-based Systems (CU 16)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4)
Microsoft SQL Server 2016 for x64-based Systems Service Pack 3 Azure Connectivity Pack

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29143
URL	https://support.microsoft.com/en-us/help/5014351
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29143
URL	https://support.microsoft.com/en-us/help/5014356
URL	https://support.microsoft.com/en-us/help/5014354
URL	https://support.microsoft.com/en-us/help/5014365
URL	https://support.microsoft.com/en-us/help/5014553
URL	https://support.microsoft.com/en-us/help/5014165
URL	https://support.microsoft.com/en-us/help/5015371
URL	https://support.microsoft.com/en-us/help/5014353
URL	https://support.microsoft.com/en-us/help/5014355
URL	https://support.microsoft.com/en-us/help/5014164

MS22-JUN: Microsoft Windows Security Update High

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2022-21166 - Intel: CVE-2022-21166 Device Register Partial Write (DRPW)
CVE-2022-21127 - Intel: CVE-2022-21127 Special Register Buffer Data Sampling Update (SRBDS Update)
CVE-2022-21123 - Intel: CVE-2022-21123 Shared Buffers Data Read (SBDR)
CVE-2022-21125 - Intel: CVE-2022-21125 Shared Buffers Data Sampling (SBDS)
CVE-2022-29111 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-29149 - Azure Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability
CVE-2022-22018 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-22021 - Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability
CVE-2022-30131 - Windows Container Isolation FS Filter Driver Elevation of Privilege Vulnerability
CVE-2022-30132 - Windows Container Manager Service Elevation of Privilege Vulnerability
ADV220002 - Microsoft Guidance on Intel Processor MMIO Stale Data Vulnerabilities
CVE-2022-30135 - Windows Media Center Elevation of Privilege Vulnerability
CVE-2022-30136 - Windows Network File System Remote Code Execution Vulnerability
CVE-2022-30137 - Azure Service Fabric Container Elevation of Privilege Vulnerability
CVE-2022-30140 - Windows iSCSI Discovery Service Remote Code Execution Vulnerability
CVE-2022-30141 - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30142 - Windows File History Remote Code Execution Vulnerability
CVE-2022-30143 - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30145 - Windows Encrypting File System (EFS) Remote Code Execution Vulnerability
CVE-2022-30148 - Windows Desired State Configuration (DSC) Information Disclosure Vulnerability
CVE-2022-30149 - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30150 - Windows Defender Remote Credential Guard Elevation of Privilege Vulnerability
CVE-2022-30151 - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2022-30152 - Windows Network Address Translation (NAT) Denial of Service Vulnerability
CVE-2022-30153 - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30154 - Microsoft File Server Shadow Copy Agent Service (RVSS) Elevation of Privilege Vulnerability
CVE-2022-30155 - Windows Kernel Denial of Service Vulnerability
CVE-2022-30160 - Windows Advanced Local Procedure Call Elevation of Privilege Vulnerability
CVE-2022-30161 - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30162 - Windows Kernel Information Disclosure Vulnerability
CVE-2022-30163 - Windows Hyper-V Remote Code Execution Vulnerability
CVE-2022-30164 - Kerberos AppContainer Security Feature Bypass Vulnerability
CVE-2022-30167 - AV1 Video Extension Remote Code Execution Vulnerability
CVE-2022-30177 - Azure RTOS GUIX Studio Remote Code Execution Vulnerability
CVE-2022-30178 - Azure RTOS GUIX Studio Remote Code Execution Vulnerability
CVE-2022-30179 - Azure RTOS GUIX Studio Remote Code Execution Vulnerability
CVE-2022-30180 - Azure RTOS GUIX Studio Information Disclosure Vulnerability
CVE-2022-30184 - .NET and Visual Studio Information Disclosure Vulnerability
CVE-2022-30188 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-29119 - HEVC Video Extensions Remote Code Execution Vulnerability

CVE-2022-30139 - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30146 - Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability
CVE-2022-30147 - Windows Installer Elevation of Privilege Vulnerability
CVE-2022-30165 - Windows Kerberos Elevation of Privilege Vulnerability
CVE-2022-30166 - Local Security Authority Subsystem Service Elevation of Privilege Vulnerability
CVE-2022-30168 - Microsoft Photos App Remote Code Execution Vulnerability
CVE-2022-30189 - Windows Autopilot Device Management and Enrollment Client Spoofing Vulnerability
CVE-2022-30190 - Microsoft Windows Support Diagnostic Tool Remote Code Execution Vulnerability
CVE-2022-32230 - Windows SMB Denial of Service Vulnerability
CVE-2022-30193 - AV1 Video Extension Remote Code Execution Vulnerability
CVE-2022-2007 - Chromium: CVE-2022-2007 Use after free in WebGPU
CVE-2022-2008 - Chromium: CVE-2022-2008 Out of bounds memory access in WebGL
CVE-2022-2010 - Chromium: CVE-2022-2010 Out of bounds read in compositing
CVE-2022-2011 - Chromium: CVE-2022-2011 Use after free in ANGLE

Affected Products:
.NET 6.0
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Azure Automation State Configuration, DSC Extension
Windows Server 2022
Windows Server 2019
Windows 10 Version 20H2 for ARM64-based Systems
Azure Automation Update Management
Windows Server 2012 (Server Core installation)
Windows Server, version 20H2 (Server Core Installation)
Windows Server 2022 Azure Edition Core Hotpatch
Windows 10 Version 21H2 for 32-bit Systems
Windows Server 2019 (Server Core installation)
Windows Server 2022 (Server Core installation)
Windows Server 2016
AV1 Video Extension
Visual Studio 2022 for Mac version 17.0
.NET Core 3.1
Azure Security Center
Windows 10 Version 21H2 for x64-based Systems
Microsoft Photos
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Visual Studio 2019 for Mac version 8.10
Windows 10 Version 1607 for 32-bit Systems
Azure Real Time Operating System GUIX

Windows 11 for x64-based Systems
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
Microsoft Visual Studio 2022 version 17.0
System Center Operations Manager (SCOM) 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows RT 8.1
Windows Server 2012 R2
Microsoft Edge (Chromium-based)
HEVC Video Extensions
Windows 10 Version 1809 for x64-based Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
NuGet.exe
System Center Operations Manager (SCOM) 2019
Log Analytics Agent
Azure Stack Hub
Windows 10 Version 21H1 for 32-bit Systems
Azure Diagnostics (LAD)
Windows 11 for ARM64-based Systems
Windows 10 for 32-bit Systems
Container Monitoring Solution
System Center Operations Manager (SCOM) 2022
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Windows 7 for x64-based Systems Service Pack 1
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Azure Real Time Operating System
Azure Sentinel
Windows 10 Version 21H1 for ARM64-based Systems
Microsoft Visual Studio 2022 version 17.2
Azure Service Fabric
Windows Server 2008 for x64-based Systems Service Pack 2
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 for x64-based Systems
HEVC Video Extension
Azure Open Management Infrastructure
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2012
Windows 10 Version 21H1 for x64-based Systems
Windows Server 2016 (Server Core installation)

Solution Details

Microsoft has released a fix for this flaw in their June 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30139
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30177
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-32230
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29119
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30155
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30165
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30140
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30149
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30178
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30188
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30135
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30184
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30150
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29149
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21127
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21123
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30160
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30180
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30141
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22018
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30137
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30154

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30193
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30189
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21166
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30162
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30179
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30147
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30164
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30131
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30168
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21125
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29111
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30143
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30166
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30152
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30136
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30142
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30153
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30161
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30148
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30132
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30163
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30146
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30167
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30151

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22021
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2010
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2011
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2007
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-2008
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30190
URL	https://support.microsoft.com/en-us/help/5014748
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30145
URL	https://support.microsoft.com/en-us/help/5013942
URL	https://support.microsoft.com/en-us/help/5014747
URL	https://support.microsoft.com/en-us/help/5014699
URL	https://support.microsoft.com/en-us/help/5015424
URL	https://support.microsoft.com/en-us/help/5014746
URL	https://support.microsoft.com/en-us/help/5014702
URL	https://support.microsoft.com/en-us/help/5015429
URL	https://support.microsoft.com/en-us/help/5014697
URL	https://support.microsoft.com/en-us/help/5014677
URL	https://support.microsoft.com/en-us/help/5014678
URL	https://support.microsoft.com/en-us/help/5014742
URL	https://support.microsoft.com/en-us/help/5014743
URL	https://support.microsoft.com/en-us/help/5014738
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30160
URL	https://support.microsoft.com/en-us/help/5014752

Type	Reference
URL	https://support.microsoft.com/en-us/help/5013941
URL	https://support.microsoft.com/en-us/help/5014710
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21123
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21127
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30135
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22021
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29149
URL	https://support.microsoft.com/en-us/help/5013943
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30150
URL	https://support.microsoft.com/en-us/help/5013945
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30184
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30188
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30178
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30149
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30165
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30140
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2011

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2008
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2007
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30139
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-2010
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30155
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30177
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-32230
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29119
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV220002
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30167
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30151
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30163
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30146
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30148
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30132
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30161

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30153
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30142
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30136
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21125
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29111
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30143
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30166
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30152
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30168
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30164
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30131
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30147
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30162
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30179
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30193
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30189

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21166
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22018
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30154
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30137
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30180
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30141
URL	https://support.microsoft.com/en-us/help/5014692
URL	https://support.microsoft.com/en-us/help/5014741
URL	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

MS22-MAR: Microsoft Internet Explorer Security Update High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their March 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2022-21977 - Media Foundation Information Disclosure Vulnerability
CVE-2022-22010 - Media Foundation Information Disclosure Vulnerability
CVE-2022-23299 - Windows PDEV Elevation of Privilege Vulnerability
CVE-2022-24502 - Windows HTML Platforms Security Feature Bypass Vulnerability
CVE-2022-23283 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2022-23285 - Remote Desktop Client Remote Code Execution Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1909 for x64-based Systems
Windows Server 2022 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1607 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Windows 10 Version 21H1 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 1909 for 32-bit Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows 11 for x64-based Systems
Windows Server 2016
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 21H2 for x64-based Systems
Windows Server 2022
Windows 10 Version 21H1 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows RT 8.1
Windows 8.1 for x64-based systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 for x64-based Systems
Windows 10 for 32-bit Systems
Windows Server 2016 (Server Core installation)
Windows Server 2012
Windows Server 2019
Windows 11 for ARM64-based Systems
Windows 10 Version 21H2 for 32-bit Systems
Windows 8.1 for 32-bit systems
Windows Server 2022 Azure Edition Core Hotpatch
Windows 10 Version 20H2 for x64-based Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows Server 2012 R2
Windows 10 Version 21H1 for 32-bit Systems
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1909 for ARM64-based Systems
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 20H2 for ARM64-based Systems
Windows Server, version 20H2 (Server Core Installation)

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23283
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23299
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21977
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22010
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24502
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23285
URL	https://support.microsoft.com/en-us/help/5011527
URL	https://support.microsoft.com/en-us/help/5011560
URL	https://support.microsoft.com/en-us/help/5011535
URL	https://support.microsoft.com/en-us/help/5011486
URL	https://support.microsoft.com/en-us/help/5011485
URL	https://support.microsoft.com/en-us/help/5011552
URL	https://support.microsoft.com/en-us/help/5011487
URL	https://support.microsoft.com/en-us/help/5011525
URL	https://support.microsoft.com/en-us/help/5010386
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21977
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23285
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22010
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24502
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23283
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23299

Type	Reference
URL	https://support.microsoft.com/en-us/help/5011495
URL	https://support.microsoft.com/en-us/help/5011529
URL	https://support.microsoft.com/en-us/help/5011491
URL	https://support.microsoft.com/en-us/help/5011564
URL	https://support.microsoft.com/en-us/help/5011580
URL	https://support.microsoft.com/en-us/help/5011534
URL	https://support.microsoft.com/en-us/help/5011497
URL	https://support.microsoft.com/en-us/help/5011503
URL	https://support.microsoft.com/en-us/help/5011493

MS22-MAR: Microsoft Windows Security Update — High

Solution Details

Microsoft has released a fix for this flaw in their March 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2022-21967 - Xbox Live Auth Manager for Windows Elevation of Privilege Vulnerability
CVE-2022-21975 - Windows Hyper-V Denial of Service Vulnerability
CVE-2022-21990 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2022-23265 - Microsoft Defender for IoT Remote Code Execution Vulnerability
CVE-2022-23266 - Microsoft Defender for IoT Elevation of Privilege Vulnerability
CVE-2022-23290 - Windows Inking COM Elevation of Privilege Vulnerability
CVE-2022-23291 - Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-23293 - Windows Fast FAT File System Driver Elevation of Privilege Vulnerability
CVE-2022-23294 - Windows Event Tracing Remote Code Execution Vulnerability
CVE-2022-23295 - Raw Image Extension Remote Code Execution Vulnerability
CVE-2022-23296 - Windows Installer Elevation of Privilege Vulnerability
CVE-2022-23298 - Windows NT OS Kernel Elevation of Privilege Vulnerability
CVE-2022-23300 - Raw Image Extension Remote Code Execution Vulnerability
CVE-2022-23301 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-22006 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-22007 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-24451 - VP9 Video Extensions Remote Code Execution Vulnerability

CVE-2022-24452 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-24453 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-24501 - VP9 Video Extensions Remote Code Execution Vulnerability
CVE-2022-24454 - Windows Security Support Provider Interface Elevation of Privilege Vulnerability
CVE-2022-24503 - Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2022-24455 - Windows CD-ROM Driver Elevation of Privilege Vulnerability
CVE-2022-24456 - HEVC Video Extensions Remote Code Execution Vulnerability
CVE-2022-24457 - HEIF Image Extensions Remote Code Execution Vulnerability
CVE-2022-24506 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-24507 - Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability
CVE-2022-24459 - Windows Fax and Scan Service Elevation of Privilege Vulnerability
CVE-2022-24512 - .NET and Visual Studio Remote Code Execution Vulnerability
CVE-2022-24464 - .NET and Visual Studio Denial of Service Vulnerability
CVE-2022-24465 - Microsoft Intune Portal for iOS Security Feature Bypass Vulnerability
CVE-2022-24515 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-24467 - Azure Site Recovery Remote Code Execution Vulnerability
CVE-2022-24522 - Skype Extension for Chrome Information Disclosure Vulnerability
CVE-2022-21973 - Windows Media Center Update Denial of Service Vulnerability
CVE-2022-23253 - Point-to-Point Tunneling Protocol Denial of Service Vulnerability
CVE-2022-23278 - Microsoft Defender for Endpoint Spoofing Vulnerability
CVE-2022-23281 - Windows Common Log File System Driver Information Disclosure Vulnerability
CVE-2022-23282 - Paint 3D Remote Code Execution Vulnerability
CVE-2022-23284 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-23286 - Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability
CVE-2022-23287 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2022-23288 - Windows DWM Core Library Elevation of Privilege Vulnerability
CVE-2022-23297 - Windows NT Lan Manager Datagram Receiver Driver Information Disclosure Vulnerability
CVE-2022-24505 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2022-24508 - Windows SMBv3 Client/Server Remote Code Execution Vulnerability
CVE-2022-24460 - Tablet Windows User Interface Application Elevation of Privilege Vulnerability
CVE-2022-24468 - Azure Site Recovery Remote Code Execution Vulnerability
CVE-2022-24469 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-24517 - Azure Site Recovery Remote Code Execution Vulnerability
CVE-2022-24470 - Azure Site Recovery Remote Code Execution Vulnerability
CVE-2022-24518 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-24519 - Azure Site Recovery Elevation of Privilege Vulnerability
CVE-2022-24471 - Azure Site Recovery Remote Code Execution Vulnerability
CVE-2022-24520 - Azure Site Recovery Remote Code Execution Vulnerability
CVE-2020-8927 - Brotli Library Buffer Overflow Vulnerability
CVE-2022-24525 - Windows Update Stack Elevation of Privilege Vulnerability
CVE-2022-24526 - Visual Studio Code Spoofing Vulnerability
CVE-2022-0789 - Chromium: CVE-2022-0789 Heap buffer overflow in ANGLE
CVE-2022-0790 - Chromium: CVE-2022-0790 Use after free in Cast UI
CVE-2022-0791 - Chromium: CVE-2022-0791 Use after free in Omnibox
CVE-2022-0792 - Chromium: CVE-2022-0792 Out of bounds read in ANGLE
CVE-2022-0793 - Chromium: CVE-2022-0793 Use after free in Views
CVE-2022-0794 - Chromium: CVE-2022-0794 Use after free in WebShare
CVE-2022-0795 - Chromium: CVE-2022-0795 Type Confusion in Blink Layout

CVE-2022-0796 - Chromium: CVE-2022-0796 Use after free in Media
CVE-2022-0797 - Chromium: CVE-2022-0797 Out of bounds memory access in Mojo
CVE-2022-0798 - Chromium: CVE-2022-0798 Use after free in MediaStream
CVE-2022-0799 - Chromium: CVE-2022-0799 Insufficient policy enforcement in Installer
CVE-2022-0800 - Chromium: CVE-2022-0800 Heap buffer overflow in Cast UI
CVE-2022-0801 - Chromium: CVE-2022-0801 Inappropriate implementation in HTML parser
CVE-2022-0802 - Chromium: CVE-2022-0802 Inappropriate implementation in Full screen mode
CVE-2022-0803 - Chromium: CVE-2022-0803 Inappropriate implementation in Permissions
CVE-2022-0804 - Chromium: CVE-2022-0804 Inappropriate implementation in Full screen mode
CVE-2022-0805 - Chromium: CVE-2022-0805 Use after free in Browser Switcher
CVE-2022-0806 - Chromium: CVE-2022-0806 Data leak in Canvas
CVE-2022-0807 - Chromium: CVE-2022-0807 Inappropriate implementation in Autofill
CVE-2022-0808 - Chromium: CVE-2022-0808 Use after free in Chrome OS Shell
CVE-2022-0809 - Chromium: CVE-2022-0809 Out of bounds memory access in WebXR

Affected Products:
Microsoft Defender for Endpoint for Windows on Windows 10 Version 20H2 for ARM64-based Systems
Microsoft Defender for Endpoint for Windows on Windows 10 Version 21H1 for x64-based Systems
Windows 10 Version 20H2 for ARM64-based Systems
Windows 7 for x64-based Systems Service Pack 1
Microsoft Defender for Endpoint for Windows on Windows 10 Version 20H2 for x64-based Systems
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Windows 10 Version 21H2 for 32-bit Systems
Windows 8.1 for 32-bit systems
Windows Server 2019
Microsoft Defender for Endpoint for Windows on Windows 10 Version 21H2 for 32-bit Systems
Windows 11 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows Server 2022 Azure Edition Core Hotpatch
HEVC Video Extension
Windows 10 Version 20H2 for x64-based Systems
Windows 8.1 for x64-based systems
Windows 10 Version 21H2 for ARM64-based Systems
.NET 6.0
Microsoft Defender for Endpoint for Windows on Windows 11 for ARM64-based Systems
Intune Company Portal for iOS
HEIF Image Extension
Windows 10 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows Server 2016 (Server Core installation)
Microsoft Defender for Endpoint for Windows on Windows 10 Version 20H2 for 32-bit Systems
Microsoft Defender for Endpoint for Windows on Windows 10 Version 1809 for x64-based Systems
Microsoft Defender for IoT
Microsoft Defender for Endpoint for Windows on Windows 10 Version 21H1 for ARM64-based Systems
Windows Server 2022
Windows 10 Version 21H2 for x64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Defender for Endpoint for Android
Paint 3D

Microsoft Defender for Endpoint for Windows on Windows 8.1 for 32-bit systems
Microsoft Defender for Endpoint for Windows on Windows 10 for 32-bit Systems
Windows 11 for x64-based Systems
Windows Server 2016
Microsoft Defender for Endpoint for Windows on Windows 10 Version 1809 for ARM64-based Systems
Visual Studio Code
Microsoft Defender for Endpoint for Windows on Windows Server 2012 R2 (Server Core installation)
Microsoft Defender for Endpoint for Windows on Windows Server 2019 (Server Core installation)
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Microsoft Defender for Endpoint for Windows on Windows 11 for x64-based Systems
Windows Server 2019 (Server Core installation)
Azure Site Recovery VMWare to Azure
Microsoft Defender for Endpoint for Linux
Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft Defender for Endpoint for Windows on Windows Server 2016 (Server Core installation)
Microsoft Defender for Endpoint for Windows on Windows RT 8.1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
.NET 5.0
Microsoft Defender for Endpoint for Windows on Windows 10 Version 21H2 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1909 for ARM64-based Systems
Windows Server 2012 R2
Windows 10 Version 21H1 for 32-bit Systems
Microsoft Defender for Endpoint for Windows on Windows Server 2022
Microsoft Defender for Endpoint for Windows on Windows Server 2022 (Server Core installation)
Windows Server, version 20H2 (Server Core Installation)
Microsoft Defender for Endpoint for Windows on Windows 10 Version 1909 for 32-bit Systems
Microsoft Defender for Endpoint for Mac
Microsoft Visual Studio 2022 version 17.0
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1607 for x64-based Systems
Microsoft Edge (Chromium-based)
Remote Desktop client for Windows Desktop
Windows RT 8.1
Microsoft Defender for Endpoint for Windows on Windows 8.1 for x64-based systems
Windows Server 2012
Skype Extension for Chrome
Microsoft Defender for Endpoint for Windows on Windows 10 Version 1909 for ARM64-based Systems
Windows 10 for 32-bit Systems
VP9 Video Extensions
Windows 10 Version 21H1 for x64-based Systems
.NET Core 3.1
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft Defender for Endpoint for Windows on Windows 10 Version 1909 for x64-based Systems
Windows 10 Version 20H2 for 32-bit Systems
Microsoft Defender for Endpoint for Windows on Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 1909 for 32-bit Systems
Microsoft Defender for Endpoint for Windows on Windows Server 2019

HEVC Video Extensions
Microsoft Defender for Endpoint for Windows on Windows Server 2022 Azure Edition Core Hotpatch
Windows 7 for 32-bit Systems Service Pack 1
Microsoft Defender for Endpoint for Windows on Windows 10 Version 1607 for 32-bit Systems
Microsoft Defender for Endpoint for Windows on Windows 10 Version 21H2 for ARM64-based Systems
Microsoft Defender for Endpoint for Windows on Windows 10 Version 1607 for x64-based Systems
Microsoft Visual Studio 2019 version 16.7 (includes 16.0 �" 16.6)
Windows 10 Version 1607 for 32-bit Systems
Windows Server 2012 (Server Core installation)
Microsoft Defender for Endpoint for Windows on Windows 10 Version 21H1 for 32-bit Systems
Microsoft Defender for Endpoint for Windows on Windows 10 Version 1809 for 32-bit Systems
Raw Image Extension
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows 10 Version 1809 for 32-bit Systems
Microsoft Defender for Endpoint for Windows on Windows Server 2012 R2
Windows 10 Version 21H1 for ARM64-based Systems
Windows 10 Version 1909 for x64-based Systems
Windows Server 2022 (Server Core installation)
Microsoft Defender for Endpoint for Windows on Windows Server 2016
Microsoft Defender for Endpoint for Windows on Windows 10 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0802
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0800
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0790
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0809
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0799
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0792
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0807
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0797
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0806
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0796

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23295
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23265
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23291
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23301
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24517
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24525
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21990
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23253
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24520
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21973
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24454
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23298
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23300
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23282
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23290
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23286
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24467
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24507
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24459
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24456
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24460
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23297
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23284
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24453

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24452
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24515
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24508
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24468
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21967
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22006
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24518
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24505
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24465
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24501
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21975
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23278
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23281
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22007
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24464
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24526
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23288
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23293
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24457
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24522
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23296
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23266
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24469
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23287

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24506
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23294
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24503
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24471
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24470
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24519
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24512
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24451
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24455
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-8927
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0798
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0808
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0789
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0793
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0803
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0795
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0805
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0801
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0791
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0794
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0804
URL	https://support.microsoft.com/en-us/help/5011495
URL	https://support.microsoft.com/en-us/help/5011529
URL	https://support.microsoft.com/en-us/help/5011491

Type	Reference
URL	https://support.microsoft.com/en-us/help/5011527
URL	https://support.microsoft.com/en-us/help/5011560
URL	https://support.microsoft.com/en-us/help/5011535
URL	https://support.microsoft.com/en-us/help/5011552
URL	https://support.microsoft.com/en-us/help/5011487
URL	https://support.microsoft.com/en-us/help/5011525
URL	https://support.microsoft.com/en-us/help/5011485
URL	https://support.microsoft.com/en-us/help/5011564
URL	https://support.microsoft.com/en-us/help/5011580
URL	https://support.microsoft.com/en-us/help/5011534
URL	https://support.microsoft.com/en-us/help/5011497
URL	https://support.microsoft.com/en-us/help/5011503
URL	https://support.microsoft.com/en-us/help/5011493
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0809
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0806
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23287
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24506
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24469
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23294
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0797

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24471
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24503
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24470
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24519
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0804
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0798
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24451
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24512
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24455
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0802
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0795
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-8927
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23278
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23281
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21975
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0793

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22007
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0800
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24464
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23288
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23293
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24526
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0801
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24457
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23266
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24522
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23296
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24456
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24460
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24459
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0808
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0792

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0805
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23297
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24452
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23284
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24453
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0794
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24508
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24468
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24515
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0807
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21967
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22006
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0796
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24505
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24465
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0799

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24518
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24501
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23265
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0791
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23295
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0789
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23291
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23301
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24517
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24525
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21990
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21973
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0803
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23253
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24520
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23282

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-0790
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24454
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23300
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23298
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23290
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23286
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24507
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24467

MS22-MAY: Microsoft Windows Security Update — High

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their May 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2022-21972 - Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-22713 - Windows Hyper-V Denial of Service Vulnerability
CVE-2022-23267 - .NET and Visual Studio Denial of Service Vulnerability
CVE-2022-23270 - Point-to-Point Tunneling Protocol Remote Code Execution Vulnerability
CVE-2022-24466 - Windows Hyper-V Security Feature Bypass Vulnerability
CVE-2022-26913 - Windows Authentication Security Feature Bypass Vulnerability
CVE-2022-26925 - Windows LSA Spoofing Vulnerability

CVE-2022-26926 - Windows Address Book Remote Code Execution Vulnerability
CVE-2022-26927 - Windows Graphics Component Remote Code Execution Vulnerability
CVE-2022-26930 - Windows Remote Access Connection Manager Information Disclosure Vulnerability
CVE-2022-26931 - Windows Kerberos Elevation of Privilege Vulnerability
CVE-2022-26932 - Storage Spaces Direct Elevation of Privilege Vulnerability
CVE-2022-26933 - Windows NTFS Information Disclosure Vulnerability
CVE-2022-26934 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2022-26935 - Windows WLAN AutoConfig Service Information Disclosure Vulnerability
CVE-2022-26936 - Windows Server Service Information Disclosure Vulnerability
CVE-2022-26937 - Windows Network File System Remote Code Execution Vulnerability
CVE-2022-26938 - Storage Spaces Direct Elevation of Privilege Vulnerability
CVE-2022-26939 - Storage Spaces Direct Elevation of Privilege Vulnerability
CVE-2022-26940 - Remote Desktop Protocol Client Information Disclosure Vulnerability
CVE-2022-22011 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2022-22012 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-22013 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-22014 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-22015 - Windows Remote Desktop Protocol (RDP) Information Disclosure Vulnerability
CVE-2022-22016 - Windows PlayToManager Elevation of Privilege Vulnerability
CVE-2022-22017 - Remote Desktop Client Remote Code Execution Vulnerability
CVE-2022-29102 - Windows Failover Cluster Information Disclosure Vulnerability
CVE-2022-29103 - Windows Remote Access Connection Manager Elevation of Privilege Vulnerability
CVE-2022-29104 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-29105 - Microsoft Windows Media Foundation Remote Code Execution Vulnerability
CVE-2022-29106 - Windows Hyper-V Shared Virtual Disk Elevation of Privilege Vulnerability
CVE-2022-29112 - Windows Graphics Component Information Disclosure Vulnerability
CVE-2022-29113 - Windows Digital Media Receiver Elevation of Privilege Vulnerability
CVE-2022-29114 - Windows Print Spooler Information Disclosure Vulnerability
CVE-2022-29115 - Windows Fax Service Remote Code Execution Vulnerability
CVE-2022-29117 - .NET and Visual Studio Denial of Service Vulnerability
CVE-2022-29125 - Windows Push Notifications Apps Elevation of Privilege Vulnerability
CVE-2022-29126 - Tablet Windows User Interface Application Core Elevation of Privilege Vulnerability
CVE-2022-29127 - BitLocker Security Feature Bypass Vulnerability
CVE-2022-29128 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29129 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29130 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29131 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29132 - Windows Print Spooler Elevation of Privilege Vulnerability
CVE-2022-29133 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-29134 - Windows Clustered Shared Volume Information Disclosure Vulnerability
CVE-2022-29135 - Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability
CVE-2022-29137 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29138 - Windows Clustered Shared Volume Elevation of Privilege Vulnerability
CVE-2022-29139 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29140 - Windows Print Spooler Information Disclosure Vulnerability
CVE-2022-29141 - Windows LDAP Remote Code Execution Vulnerability
CVE-2022-29142 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2022-29145 - .NET and Visual Studio Denial of Service Vulnerability
CVE-2022-29148 - Visual Studio Remote Code Execution Vulnerability

CVE-2022-22019 - Remote Procedure Call Runtime Remote Code Execution Vulnerability
CVE-2022-29972 - Insight Software: CVE-2022-29972 Magnitude Simba Amazon Redshift ODBC Driver
CVE-2022-23279 - Windows ALPC Elevation of Privilege Vulnerability
CVE-2022-26923 - Active Directory Domain Services Elevation of Privilege Vulnerability
CVE-2022-29116 - Windows Kernel Information Disclosure Vulnerability
CVE-2022-29120 - Windows Clustered Shared Volume Information Disclosure Vulnerability
CVE-2022-29121 - Windows WLAN AutoConfig Service Denial of Service Vulnerability
CVE-2022-29122 - Windows Clustered Shared Volume Information Disclosure Vulnerability
CVE-2022-29123 - Windows Clustered Shared Volume Information Disclosure Vulnerability
CVE-2022-29150 - Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability
CVE-2022-29151 - Windows Cluster Shared Volume (CSV) Elevation of Privilege Vulnerability
ADV220001 - Upcoming improvements to Azure Data Factory and Azure Synapse Pipeline infrastructure in response to CVE-2022-29972
CVE-2022-30129 - Visual Studio Code Remote Code Execution Vulnerability

Affected Products:
Windows Server 2012
Windows Server 2022
Windows 11 for x64-based Systems
Windows 10 Version 20H2 for x64-based Systems
Microsoft Visual Studio 2022 version 17.1
Microsoft Visual Studio 2019 version 16.9 (includes 16.0 - 16.8)
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows Server 2016 (Server Core installation)
Azure Synapse
Azure Data Factory
Windows 10 Version 21H2 for 32-bit Systems
Windows 10 Version 21H1 for ARM64-based Systems
Windows Server 2019 (Server Core installation)
Windows Server 2019
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8)
Windows 10 Version 20H2 for ARM64-based Systems
Microsoft Visual Studio 2022 version 17.0
Windows 11 for ARM64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1909 for ARM64-based Systems
Windows Server 2012 (Server Core installation)
Windows 10 Version 1909 for 32-bit Systems
Windows 10 Version 21H2 for ARM64-based Systems
Windows 10 for x64-based Systems
.NET Core 3.1
Visual Studio Code
.NET 5.0
Windows 10 for 32-bit Systems
Windows Server 2016

.NET 6.0
Windows 8.1 for x64-based systems
Windows 10 Version 21H1 for x64-based Systems
Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10)
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server, version 20H2 (Server Core Installation)
Windows 10 Version 20H2 for 32-bit Systems
Windows 10 Version 21H2 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Remote Desktop client for Windows Desktop
Windows 8.1 for 32-bit systems
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2012 R2
Windows 10 Version 1909 for x64-based Systems
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1
Windows Server 2012 R2 (Server Core installation)
Windows Server 2008 for x64-based Systems Service Pack 2
Self-hosted Integration Runtime
Windows Server 2022 (Server Core installation)
Windows 10 Version 21H1 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29134
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29131
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29133
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29122
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26939
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23270
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22017
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29135
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29126
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29142

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26938
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29130
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29120
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29141
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23267
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29145
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21972
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29127
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26940
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29151
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29148
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22012
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26923
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26932
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29113
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29129
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29115
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26925
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26935
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29112
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22011
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29104
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26933
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29139

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26931
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22013
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22015
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29137
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29106
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-24466
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26930
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29114
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29102
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-23279
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29138
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29116
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26926
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26936
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29972
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22014
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26934
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29103
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29150
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29128
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22016
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29105
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29125
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26913

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29132
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30129
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29123
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22713
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29121
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29117
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29140
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26927
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-26937
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-22019
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23267
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-21972
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29141
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29134
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29120
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29145
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29142
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29126
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29130

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26938
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29131
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22019
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26937
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22017
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29135
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23270
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26939
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29133
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29122
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22713
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30129
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29132
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26913
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29123
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29125

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29117
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29140
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26927
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29121
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22014
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29972
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26936
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22016
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29105
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV220001
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29128
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29103
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26934
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29150
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29138
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29114

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-23279
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29102
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26930
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-24466
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29116
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26926
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29139
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29112
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26933
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29104
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22011
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26935
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22015
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29106
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29137
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26931

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22013
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-22012
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29148
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29127
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29151
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26940
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29115
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26925
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29129
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26923
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-26932
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-29113
URL	https://support.microsoft.com/en-us/help/5013942
URL	https://support.microsoft.com/en-us/help/5014326
URL	https://support.microsoft.com/en-us/help/5013945
URL	https://support.microsoft.com/en-us/help/5014012
URL	https://support.microsoft.com/en-us/help/5013943
URL	https://support.microsoft.com/en-us/help/5014011

Type	Reference
URL	https://support.microsoft.com/en-us/help/5014001
URL	https://support.microsoft.com/en-us/help/5014017
URL	https://support.microsoft.com/en-us/help/5014010
URL	https://support.microsoft.com/en-us/help/5013999
URL	https://support.microsoft.com/en-us/help/5014329
URL	https://support.microsoft.com/en-us/help/5013941
URL	https://support.microsoft.com/en-us/help/5013944
URL	https://support.microsoft.com/en-us/help/5014018
URL	https://support.microsoft.com/en-us/help/5014025
URL	https://support.microsoft.com/en-us/help/5013963
URL	https://support.microsoft.com/en-us/help/5013952
URL	https://support.microsoft.com/en-us/help/5014006
URL	https://insightsoftware.com/trust/security/advisories/redshift-and-athena-driver-vulnerability/

OpenSSH 'kbdint_next_device' Function Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5600
BUGTRAQ	http://www.securityfocus.com/bid/92012
BUGTRAQ	http://www.securityfocus.com/bid/75990
BUGTRAQ	http://www.securityfocus.com/bid/91787
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05128992
URL	http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04952480
URL	http://www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10157
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
URL	http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth2-chall.c.diff?r1=1.42&r2=1.43&f=h
URL	http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/auth2-chall.c
URL	https://security.netapp.com/advisory/ntap-20151106-0001/
URL	https://support.apple.com/kb/HT205031
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10697

OpenSSH Security Bypass Vulnerability High

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

Vulnerability Details

The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10012
BUGTRAQ	http://www.securityfocus.com/bid/94975
URL	http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.647637
URL	https://www.openssh.com/txt/release-7.4
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03818en_us
URL	https://security.netapp.com/advisory/ntap-20171130-0002/
URL	https://github.com/openbsd/src/commit/3095060f479b86288e31c79ecbc5131a66bcd2f9
URL	https://cwe.mitre.org/data/definitions/119.html

OpenSSH 'session.c' Local Security Bypass Vulnerability — High

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

Vulnerability Details

The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8325
BUGTRAQ	http://www.securityfocus.com/bid/86187
URL	https://anongit.mindrot.org/openssh.git/commit/?id=85bdcd7c92fe7ff133bbc4e10a65c91810f88755
URL	https://security-tracker.debian.org/tracker/CVE-2015-8325
URL	https://security.netapp.com/advisory/ntap-20180628-0001/
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1328012
URL	https://people.canonical.com/~ubuntu-security/cve/2015/CVE-2015-8325.html

OpenSSH 'ssh-agent.c' Untrusted Search Path Vulnerability High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10009
BUGTRAQ	http://www.securityfocus.com/bid/94968

Type	Reference
URL	https://cwe.mitre.org/data/definitions/426.html
URL	https://bugs.chromium.org/p/project-zero/issues/detail?id=1009
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03818en_us
URL	https://security.netapp.com/advisory/ntap-20171130-0002/
URL	http://packetstormsecurity.com/files/140261/OpenSSH-Arbitrary-Library-Loading.html
URL	https://www.openssh.com/txt/release-7.4
URL	http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.647637
URL	https://github.com/openbsd/src/commit/9476ce1dd37d3c3218d5640b74c34c65e5f4efe5

OpenSSH 'ssh-agent' Double Free Vulnerability High

Solution Details

Use of rsync in the place of scp for better security. If scp is required, please ensure it is updated with the latest patches and fixes from the vendor.

Vulnerability Details

ssh-agent in OpenSSH has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.
Impact:
An attacker could leverage this vulnerability to cause a program's memory management data structures to become corrupted and could allow a malicious user to write values in arbitrary memory spaces.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.6

CVSS Vector: AV:N/AC:H/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28041

Type	Reference
URL	https://github.com/openssh/openssh-portable/commit/e04fd6dde16de1cdc5a4d9946397ff60d96568db
URL	https://www.openssh.com/

OpenSSH 'ssh/kex.c' Denial of Service Vulnerability

High

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

Vulnerability Details

The kex_input_kexinit function in kex.c in OpenSSH 6.x and 7.x through 7.3 allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate KEXINIT requests.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-8858
BUGTRAQ	http://www.securityfocus.com/bid/93776
URL	https://ftp.openbsd.org/pub/OpenBSD/patches/6.0/common/013_ssh_kexinit.patch.sig
URL	http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/kex.c.diff?r1=1.126&r2=1.127&f=h
URL	http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/kex.c?rev=1.127&content-type=text/x-cvsweb-markup
URL	https://github.com/dag-erling/kexkill/issues/1
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1384860
URL	https://security.netapp.com/advisory/ntap-20180201-0001/
URL	https://cwe.mitre.org/data/definitions/399.html

Type	Reference
URL	https://github.com/openssh/openssh-portable/commit/ec165c392ca54317dbe3064a8c200de6531e89ad

OpenSSH X11 Forwarding Access Bypass — High

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1908
BUGTRAQ	http://www.securityfocus.com/bid/84427
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	http://www.openssh.com/txt/release-7.2
URL	https://anongit.mindrot.org/openssh.git/commit/?id=ed4ce82dbfa8a3a3c8ea6fa0db113c71e234416c
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1298741

PHP bcmath.c 'bcpowmod' Modified Data Structure Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 modifies certain data structures without considering whether they are copies of the _zero_, _one_, or _two_ global variable, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4538
BUGTRAQ	http://www.securityfocus.com/bid/90173
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-7.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://git.php.net/?p=php-src.git;a=commit;h=d650063a0457aec56364e4005a636dc6c401f9cd
URL	https://bugs.php.net/bug.php?id=72093

PHP bcmath.c 'bcpowmod' Negative Integer Denial of Service High

Vulnerability Details

The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 accepts a negative integer for the scale argument, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4537
BUGTRAQ	http://www.securityfocus.com/bid/90173
URL	http://php.net/ChangeLog-7.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://git.php.net/?p=php-src.git;a=commit;h=d650063a0457aec56364e4005a636dc6c401f9cd
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=72093
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731

PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 'get_icu_value_internal' Function Denial of Service

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The get_icu_value_internal function in ext/intl/locale/locale_methods.c in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 does not ensure the presence of a '\0' character, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted locale_get_primary_language call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5093
BUGTRAQ	http://www.securityfocus.com/bid/90946
URL	https://github.com/php/php-src/commit/97eff7eb57fc2320c267a949cffd622c38712484?w=1
URL	https://bugs.php.net/bug.php?id=72241
URL	http://php.net/ChangeLog-5.php
URL	http://php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/125.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731

PHP before 5.5.36 and 5.6.x before 5.6.22 'file.c' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Integer overflow in the fread function in ext/standard/file.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer in the second argument.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5096
BUGTRAQ	http://www.securityfocus.com/bid/90861
URL	http://php.net/ChangeLog-5.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	https://cwe.mitre.org/data/definitions/190.html
URL	https://bugs.php.net/bug.php?id=72114
URL	https://github.com/php/php-src/commit/abd159cce48f3e34f08e4751c568e09677d5ec9c?w=1

PHP before 5.5.36 and 5.6.x before 5.6.22 'php_escape_html_entities_ex' Function Denial of Service

High

Vulnerability Details

Integer overflow in the php_escape_html_entities_ex function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from a FILTER_SANITIZE_FULL_SPECIAL_CHARS filter_var call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-5094.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5095
BUGTRAQ	http://www.securityfocus.com/bid/92144
URL	https://bugs.php.net/bug.php?id=72135

Type	Reference
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/190.html
URL	https://gist.github.com/8ef775c117d84ff15185953990a28576

PHP before 5.5.36 and 5.6.x before 5.6.22 'php_html_entities' Function Denial of Service

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Integer overflow in the php_html_entities function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from the htmlspecialchars function.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5094
BUGTRAQ	http://www.securityfocus.com/bid/90857
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=72135
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	https://github.com/php/php-src/commit/0da8b8b801f9276359262f1ef8274c7812d3dfda?w=1
URL	https://cwe.mitre.org/data/definitions/190.html

PHP CGI Component Command Execution Vulnerability

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9427
BUGTRAQ	http://www.securityfocus.com/bid/71833
URL	https://support.apple.com/HT205267
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=68618
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://advisories.mageia.org/MGASA-2015-0040.html
URL	http://git.php.net/?p=php-src.git;a=commit;h=f9ad3086693fce680fbe246e4a45aa92edd2ac35

PHP 'curl_file.c' CURLFile Implementation Denial of Service

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in the CURLFile implementation in ext/curl/curl_file.c in PHP before 5.6.27 and 7.x before 7.0.12 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that is mishandled during __wakeup processing.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9137
BUGTRAQ	http://www.securityfocus.com/bid/93577
URL	http://git.php.net/?p=php-src.git;a=commit;h=0e6fe3a4c96be2d3e88389a5776f878021b4c59f
URL	https://bugs.php.net/bug.php?id=73147
URL	https://www.tenable.com/security/tns-2016-19
URL	http://www.php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/416.html

PHP 'dynamicGetbuf' Denial of Service Vulnerability

High

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

Integer signedness error in the dynamicGetbuf function in gd_io_dp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted imagecreatefromstring call.
Impact:
An attacker can exploit this issue to create a denial-of-service condition. Due to the nature of this issue, arbitrary code execution may be possible but this has not been confirmed.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-8670
BUGTRAQ	http://www.securityfocus.com/bid/93594
URL	http://www.php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=73280
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://github.com/libgd/libgd/commit/53110871935244816bbb9d131da0bccff734bfe9
URL	http://php.net/downloads.php

PHP 'enchant_broker_request_dict' Function Arbitrary Code Execution

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Heap-based buffer overflow in the enchant_broker_request_dict function in ext/enchant/enchant.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allows remote attackers to execute arbitrary code via vectors that trigger creation of multiple dictionaries.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9705
BUGTRAQ	http://www.securityfocus.com/bid/73031
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference
URL	http://svn.php.net/viewvc/pecl/enchant/trunk/enchant.c?r1=317600&r2=335803
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=68552
URL	https://www.htbridge.com/advisory/HTB23252
URL	http://php.net/ChangeLog-5.php
URL	https://support.apple.com/HT205267

PHP 'escapeshellarg' Function Remote Command Execution Vulnerability — High

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The escapeshellarg function in ext/standard/exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4642
BUGTRAQ	http://www.securityfocus.com/bid/75290
URL	http://php.net/ChangeLog-5.php

Type	Reference
URL	http://git.php.net/?p=php-src.git;a=commit;h=d2ac264ffea5ca2e85640b6736e0c7cd4ee9a4a9
URL	https://cwe.mitre.org/data/definitions/78.html
URL	https://bugs.php.net/bug.php?id=69646

PHP exif.c 'exif_process_IFD_in_JPEG' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exif_process_IFD_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate IFD sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4543
BUGTRAQ	http://www.securityfocus.com/bid/89844
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://git.php.net/?p=php-src.git;a=commit;h=082aecfc3a753ad03be82cf14f03ac065723ec92
URL	https://bugs.php.net/bug.php?id=72094
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722

Type	Reference
URL	http://php.net/ChangeLog-7.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149

PHP exif.c 'exif_process_IFD_TAG' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4542
BUGTRAQ	http://www.securityfocus.com/bid/89844
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://git.php.net/?p=php-src.git;a=commit;h=082aecfc3a753ad03be82cf14f03ac065723ec92
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://bugs.php.net/bug.php?id=72094
URL	http://php.net/ChangeLog-7.php

Type	Reference
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-5.php

PHP exif.c 'exif_process_TIFF_in_JPEG' Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exif_process_TIFF_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate TIFF start data, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4544
BUGTRAQ	http://www.securityfocus.com/bid/89844
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=72094
URL	https://git.php.net/?p=php-src.git;a=commit;h=082aecfc3a753ad03be82cf14f03ac065723ec92

PHP 'exif_process_IFD_in_MAKERNOTE' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exif_process_IFD_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6291
BUGTRAQ	http://www.securityfocus.com/bid/92073
URL	https://support.apple.com/HT207170
URL	https://bugs.php.net/72603
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://php.net/ChangeLog-7.php
URL	http://php.net/ChangeLog-5.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=eebcbd5de38a0f1c2876035402cb770e37476519

PHP 'exif_process_IFD_in_TIFF' Uninitialized Read Vulnerability High

Vulnerability Details

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_TIFF.
Impact:
An attacker could leverage this vulnerability to read the contents of memory to obtain information that could aid in launching further attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of PHP.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9641
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://security.netapp.com/advisory/ntap-20190502-0007/
URL	http://php.net/downloads.php

PHP 'ext/phar/phar_object.c' Zero-length Uncompress Denial of Service

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/phar/phar_object.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 mishandles zero-length uncompressed data, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted (1) TAR, (2) ZIP, or (3) PHAR archive.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4342
BUGTRAQ	http://www.securityfocus.com/bid/89154
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-5.php
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=71354
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149

PHP 'ext/soap/soap.c' Type Confusion Vulnerability — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The SoapClient::__call method in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that __default_headers is an array, which allows remote attackers to execute arbitrary code by providing crafted serialized data with an unexpected data type, related to a "type confusion" issue.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4147
BUGTRAQ	http://www.securityfocus.com/bid/73357
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://support.apple.com/kb/HT205031
URL	https://bugs.php.net/bug.php?id=69085

Type	Reference
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://php.net/ChangeLog-5.php

PHP 'ext/spl/spl_array.c' Use-after-free Remote Code Execution — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in the SPL unserialize implementation in ext/spl/spl_array.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to execute arbitrary code via crafted serialized data that triggers misuse of an array field.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6832
URL	https://bugs.php.net/bug.php?id=70068

PHP ext/standard/http_fopen_wrapper.c 'php_stream_url_wrap_http_ex' Stack-based Buffer Under-read — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-7584
BUGTRAQ	http://www.securityfocus.com/bid/103204
URL	https://www.tenable.com/security/tns-2018-12
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=75981
URL	https://github.com/php/php-src/commit/523f230c831d7b33353203fa34aee4e92ac12bba
URL	https://www.tenable.com/security/tns-2018-03
URL	https://cwe.mitre.org/data/definitions/119.html

PHP File Extension Restriction Bypass

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4025
BUGTRAQ	http://www.securityfocus.com/bid/74904
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://support.apple.com/kb/HT205031
URL	https://bugs.php.net/bug.php?id=69418
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html

PHP Fileinfo Component 'apprentice_load' Denial of Service Flaw — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

** DISPUTED ** The apprentice_load function in libmagic/apprentice.c in the Fileinfo component in PHP through 5.6.4 attempts to perform a free operation on a stack-based character array, which allows remote attackers to cause a denial of service (memory corruption or application crash) or possibly have unspecified other impact via unknown vectors. NOTE: this is disputed by the vendor because the standard erealloc behavior makes the free operation unreachable.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9426
URL	https://bugs.php.net/bug.php?id=68665
URL	http://git.php.net/?p=php-src.git;a=commit;h=a72cd07f2983dc43a6bb35209dc4687852e53c09

Type	Reference
URL	http://git.php.net/?p=php-src.git;a=commit;h=ef89ab2f99fbd9b7b714556d4f1f50644eb54191

PHP Fileinfo Component Crafted ELF File Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9653
BUGTRAQ	http://www.securityfocus.com/bid/72516
URL	https://github.com/file/file/commit/445c8fb0ebff85195be94cd9f7e1df89cade5c7f
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html

PHP 'ftp_genlist' Function Heap Buffer Overflow — High

Vulnerability Details

Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4022
BUGTRAQ	http://www.securityfocus.com/bid/74902
URL	https://support.apple.com/kb/HT205031
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=69545
URL	http://php.net/ChangeLog-5.php

PHP 'ftp_genlist' Function LIST Command Buffer Overflow — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4022.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4643
BUGTRAQ	http://www.securityfocus.com/bid/75291
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://git.php.net/?p=php-src.git;a=commit;h=0765623d6991b62ffcd93ddb6be8a5203a2fa7e2
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://bugs.php.net/bug.php?id=69545

PHP gd.c 'imagegammacorrect' Input Validation Denial of Service Vulnerability

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7127
BUGTRAQ	http://www.securityfocus.com/bid/92757
URL	https://cwe.mitre.org/data/definitions/787.html

Type	Reference
URL	http://www.php.net/ChangeLog-7.php
URL	https://github.com/php/php-src/commit/1bd103df00f49cf4d4ade2cfe3f456ac058a4eae?w=1
URL	https://www.tenable.com/security/tns-2016-19
URL	https://bugs.php.net/bug.php?id=72730

PHP gd.c 'imagetruecolortopalette' Input Validation Denial of Service Vulnerability

High

Vulnerability Details

The imagetruecolortopalette function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate the number of colors, which allows remote attackers to cause a denial of service (select_colors allocation error and out-of-bounds write) or possibly have unspecified other impact via a large value in the third argument.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7126
BUGTRAQ	http://www.securityfocus.com/bid/92755
URL	http://www.php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=72697
URL	https://github.com/php/php-src/commit/b6f13a5ef9d6280cf984826a5de012a32c396cd4?w=1
URL	https://cwe.mitre.org/data/definitions/787.html
URL	https://www.tenable.com/security/tns-2016-19

PHP 'gd_webp.c' Denial of Service Vulnerability High

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

Integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP through 7.0.11, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted imagewebp and imagedestroy calls.
Impact:
An attacker could cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7568
BUGTRAQ	http://www.securityfocus.com/bid/93184
URL	https://github.com/libgd/libgd/issues/308
URL	https://github.com/php/php-src/commit/c18263e0e0769faee96a5d0ee04b750c442783c6
URL	https://github.com/libgd/libgd/commit/40bec0f38f50e8510f5bb71a82f516d46facde03
URL	https://bugs.php.net/bug.php?id=73003
URL	http://php.net/downloads.php
URL	https://cwe.mitre.org/data/definitions/190.html

PHP grapheme.c 'grapheme_stripos' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The grapheme_stripos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4540
BUGTRAQ	http://www.securityfocus.com/bid/90172
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	http://php.net/ChangeLog-7.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://bugs.php.net/bug.php?id=72061
URL	https://git.php.net/?p=php-src.git;a=commit;h=fd9689745c44341b1bd6af4756f324be8abba2fb
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-5.php

PHP grapheme_string.c 'graphme_strpos' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The grapheme_strpos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4541
BUGTRAQ	http://www.securityfocus.com/bid/90172
URL	https://git.php.net/?p=php-src.git;a=commit;h=fd9689745c44341b1bd6af4756f324be8abba2fb
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-7.php
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=72061
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722

PHP Heap-Based Buffer Over-Read Vulnerability — High

Vulnerability Details

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A heap-based buffer over-read in PHAR reading functions in the PHAR extension may allow an attacker to read allocated or unallocated memory past the actual data when trying to parse the file name, a different vulnerability than CVE-2018-20783. This is related to phar_detect_phar_fname_ext in ext/phar/phar.c.
Impact:
Successfully exploiting these issues allow attackers to execute arbitrary code in the affected asset or obtain sensitive information. Failed exploits will result in denial-of-service conditions.

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of PHP.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9021
BUGTRAQ	http://www.securityfocus.com/bid/107156
BUGTRAQ	http://www.securityfocus.com/bid/106747
URL	https://bugs.php.net/bug.php?id=77247
URL	http://php.net/downloads.php
URL	https://security.netapp.com/advisory/ntap-20190321-0001/
URL	https://cwe.mitre.org/data/definitions/125.html

PHP IMAP PHP Extension 'phar_fix_filepath' Function Buffer Overflow Vulnerability

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Stack-based buffer overflow in the phar_fix_filepath function in ext/phar/phar.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value, as demonstrated by mishandling of an e-mail attachment by the imap PHP extension.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5590
BUGTRAQ	http://www.securityfocus.com/bid/75970
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://bugs.php.net/bug.php?id=69923
URL	http://git.php.net/?p=php-src.git;a=commit;h=6dedeb40db13971af45276f80b5375030aa7e76f

PHP 'incomplete_class.c' Type Confusion Denial of Service — High

Vulnerability Details

The __PHP_Incomplete_Class function in ext/standard/incomplete_class.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4602
BUGTRAQ	http://www.securityfocus.com/bid/75249
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=69152
URL	http://git.php.net/?p=php-src.git;a=commit;h=fb83c76deec58f1fab17c350f04c9f042e5977d1

PHP Invalid Memory Access Vulnerability High

Vulnerability Details

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. Invalid input to the function xmlrpc_decode() can lead to an invalid memory access (heap out of bounds read or read after free). This is related to xml_elem_parse_buf in ext/xmlrpc/libxmlrpc/xml_element.c.
Impact:
Successfully exploiting these issues allow attackers to execute arbitrary code in the affected asset or obtain sensitive information. Failed exploits will result in denial-of-service conditions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of PHP.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9020
BUGTRAQ	http://www.securityfocus.com/bid/107156
URL	https://bugs.php.net/bug.php?id=77242
URL	http://php.net/downloads.php
URL	https://security.netapp.com/advisory/ntap-20190321-0001/
URL	https://bugs.php.net/bug.php?id=77249

PHP 'locale_accept_from_http' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6294
BUGTRAQ	http://www.securityfocus.com/bid/92115
URL	http://git.php.net/?p=php-src.git;a=commit;h=aa82e99ed8003c01f1ef4f0940e56b85c5b032d4
URL	https://cwe.mitre.org/data/definitions/125.html
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/72533
URL	http://php.net/ChangeLog-7.php
URL	https://support.apple.com/HT207170

PHP 'locale_methods.c' Argument Overflow Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The get_icu_disp_value_src_php function in ext/intl/locale/locale_methods.c in PHP before 5.3.29, 5.4.x before 5.4.30, and 5.5.x before 5.5.14 does not properly restrict calls to the ICU uresbund.cpp component, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a locale_get_display_name call with a long first argument.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9912
BUGTRAQ	http://www.securityfocus.com/bid/68549
URL	https://bugs.php.net/bug.php?id=67397
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1383569
URL	https://cwe.mitre.org/data/definitions/119.html

PHP mbfilter.c 'mbfl_strcut' Integer Overflows Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Multiple integer overflows in the mbfl_strcut function in ext/mbstring/libmbfl/mbfl/mbfilter.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted mb_strcut call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4073
BUGTRAQ	http://www.securityfocus.com/bid/85991
URL	https://support.apple.com/HT206567
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://www.php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=71906
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference
URL	https://gist.github.com/smalyshev/d8355c96a657cc5dba70
URL	https://git.php.net/?p=php-src.git;a=commit;h=64f42c73efc58e88671ad76b6b6bc8e2b62713e1

PHP mcrypt.c Multiple Integer Overflow Vulnerabilities — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Multiple integer overflows in mcrypt.c in the mcrypt extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted length value, related to the (1) mcrypt_generic and (2) mdecrypt_generic functions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5769
BUGTRAQ	http://www.securityfocus.com/bid/91399
URL	https://support.apple.com/HT207170
URL	https://cwe.mitre.org/data/definitions/190.html
URL	http://php.net/ChangeLog-7.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://github.com/php/php-src/commit/6c5211a0cef0cc2854eaa387e0eb036e012904d0?w=1
URL	https://bugs.php.net/bug.php?id=72455
URL	http://php.net/ChangeLog-5.php

PHP Multiple Heap-Based Buffer Over-Read Vulnerabilities — High

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of PHP.

Vulnerability Details

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. A number of heap-based buffer over-read instances are present in mbstring regular expression functions when supplied with invalid multibyte data. These occur in ext/mbstring/oniguruma/regcomp.c, ext/mbstring/oniguruma/regexec.c, ext/mbstring/oniguruma/regparse.c, ext/mbstring/oniguruma/enc/unicode.c, and ext/mbstring/oniguruma/src/utf32_be.c when a multibyte regular expression pattern contains invalid multibyte sequences.
Impact:
Successfully exploiting these issues allow attackers to execute arbitrary code in the affected asset or obtain sensitive information. Failed exploits will result in denial-of-service conditions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9023
BUGTRAQ	http://www.securityfocus.com/bid/107156
URL	https://bugs.php.net/bug.php?id=77394
URL	https://bugs.php.net/bug.php?id=77381
URL	https://bugs.php.net/bug.php?id=77382
URL	https://bugs.php.net/bug.php?id=77385
URL	https://bugs.php.net/bug.php?id=77371
URL	https://security.netapp.com/advisory/ntap-20190321-0001/
URL	https://support.f5.com/csp/article/K06372014
URL	https://bugs.php.net/bug.php?id=77370
URL	https://cwe.mitre.org/data/definitions/125.html

Type	Reference
URL	https://bugs.php.net/bug.php?id=77418
URL	http://php.net/downloads.php

PHP Multiple Type Confusion Denial of Service Vulnerabilities — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

PHP before 5.6.7 might allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in (1) ext/soap/php_encoding.c, (2) ext/soap/php_http.c, and (3) ext/soap/soap.c, a different issue than CVE-2015-4600.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4601
BUGTRAQ	http://www.securityfocus.com/bid/75246
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://git.php.net/?p=php-src.git;a=commit;h=0c136a2abd49298b66acb0cad504f0f972f5bfe8

PHP OPcache Extension '_zend_shared_memdup' Function Denial of Service Flaw — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Use-after-free vulnerability in the _zend_shared_memdup function in zend_shared_alloc.c in the OPcache extension in PHP through 5.6.7 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1351
BUGTRAQ	http://www.securityfocus.com/bid/71929
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	https://support.apple.com/HT205267
URL	https://cwe.mitre.org/data/definitions/416.html
URL	https://bugs.php.net/bug.php?id=68677
URL	http://git.php.net/?p=php-src.git;a=commit;h=777c39f4042327eac4b63c7ee87dc1c7a09a3115
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html

PHP Pathname Sanitization Remote Arbitrary File Access Vulnerability — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument save method or (2) the GD imagepsloadfont function, as demonstrated by a filename\0.html attack that bypasses an intended configuration in which client users may write to only .html files.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4598
BUGTRAQ	http://www.securityfocus.com/bid/75244
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=69719

PHP 'pcntl_exec' Implementation File Extension Restriction Bypass — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4026

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/75056
URL	http://php.net/ChangeLog-5.php
URL	https://support.apple.com/kb/HT205031
URL	https://cwe.mitre.org/data/definitions/19.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=68598

PHP phar.c 'phar_parse_pharfile' Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Off-by-one error in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted PHAR archive with an alias mismatch.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10160
BUGTRAQ	http://www.securityfocus.com/bid/95783
URL	http://php.net/ChangeLog-5.php
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	https://www.tenable.com/security/tns-2017-04
URL	http://php.net/ChangeLog-7.php

Type	Reference
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://bugs.php.net/bug.php?id=73768
URL	https://github.com/php/php-src/commit/b28b8b2fee6dfa6fcd13305c581bb835689ac3be

PHP Phar Extension 'phar_analyze_path' Arbitrary Code Execution High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The Phar extension in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via a crafted filename, as demonstrated by mishandling of \0 characters by the phar_analyze_path function in ext/phar/phar.c.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4072
BUGTRAQ	http://www.securityfocus.com/bid/85993
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	https://git.php.net/?p=php-src.git;a=commit;h=1e9b175204e3286d64dfd6c9f09151c31b5e099a
URL	https://gist.github.com/smalyshev/80b5c2909832872f2ba2
URL	https://bugs.php.net/bug.php?id=71860
URL	https://support.apple.com/HT206567

Type	Reference
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	http://www.php.net/ChangeLog-7.php

PHP phar_object.c 'phar_convert_to_other' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5589
BUGTRAQ	http://www.securityfocus.com/bid/75974
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://php.net/ChangeLog-5.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=bf58162ddf970f63502837f366930e44d6a992cf
URL	https://bugs.php.net/bug.php?id=69958

PHP 'phar_parse_metadata' Function Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The phar_parse_metadata function in ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (heap metadata corruption) or possibly have unspecified other impact via a crafted tar archive.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3307
BUGTRAQ	http://www.securityfocus.com/bid/74703
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.apple.com/kb/HT205031
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=69443
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1223441

PHP "phar_rename_archive" Function Denial of Service Flaw — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in the phar_rename_archive function in phar_object.c in PHP before 5.5.22 and 5.6.x before 5.6.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted renaming of a Phar archive to the name of an existing file.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2301
BUGTRAQ	http://www.securityfocus.com/bid/73037
URL	https://bugs.php.net/bug.php?id=68901
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1194747
URL	https://support.apple.com/HT205267
URL	http://git.php.net/?p=php-src.git;a=commit;h=b2cf3f064b8f5efef89bb084521b61318c71781b
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html

PHP 'phar_set_inode' Function Stack Buffer Overflow — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3329
BUGTRAQ	http://www.securityfocus.com/bid/74240
URL	http://git.php.net/?p=php-src.git;a=commit;h=f59b67ae50064560d7bfcdb0d6a8ab284179053c
URL	https://bugs.php.net/bug.php?id=69441
URL	http://php.net/ChangeLog-5.php
URL	https://support.apple.com/kb/HT205031
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://support.apple.com/HT205267
URL	https://cwe.mitre.org/data/definitions/119.html

PHP 'php_date.c' Multiple Use-After-Free Arbitrary Code Execution Flaws

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Multiple use-after-free vulnerabilities in ext/date/php_date.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allow remote attackers to execute arbitrary code via crafted serialized input containing a (1) R or (2) r type specifier in (a) DateTimeZone data handled by the php_date_timezone_initialize_from_hash function or (b) DateTime data handled by the php_date_initialize_from_hash function.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0273
BUGTRAQ	http://www.securityfocus.com/bid/72701
URL	http://git.php.net/?p=php-src.git;a=commit;h=71335e6ebabc1b12c057d8017fd811892ecdfd24
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://support.apple.com/HT205267
URL	https://support.apple.com/HT205375
URL	https://bugs.php.net/bug.php?id=68942
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1194730
URL	http://support.apple.com/kb/HT204942
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html

PHP php_http.c 'make_http_soap_request' Remote Code Execution High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not properly retrieve keys, which allows remote attackers to cause a denial of service (NULL pointer dereference, type confusion, and application crash) or possibly execute arbitrary code via crafted serialized data representing a numerically indexed _cookies array, related to the SoapClient::__call method in ext/soap/soap.c.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8835
BUGTRAQ	http://www.securityfocus.com/bid/84426
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=70081

PHP php_mbregex.c '_php_mb_regex_ereg_replace_exec' Double Free Vulnerability

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Double free vulnerability in the _php_mb_regex_ereg_replace_exec function in php_mbregex.c in the mbstring extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by leveraging a callback exception.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5768
BUGTRAQ	http://www.securityfocus.com/bid/91396
URL	http://github.com/php/php-src/commit/5b597a2e5b28e2d5a52fc1be13f425f08f47cb62?w=1
URL	https://support.apple.com/HT207170
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/415.html
URL	https://bugs.php.net/bug.php?id=72402

Type	Reference
URL	http://php.net/ChangeLog-7.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731

PHP 'php_snmp_error' Function Format String Arbitrary Code Execution

High

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Format string vulnerability in the php_snmp_error function in ext/snmp/snmp.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via format string specifiers in an SNMP::get call.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4071
BUGTRAQ	http://www.securityfocus.com/bid/85800
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://support.apple.com/HT206567
URL	http://www.php.net/ChangeLog-7.php
URL	https://git.php.net/?p=php-src.git;a=commit;h=6e25966544fb1d2f3d7596e060ce9c9269bbdcf8

Type	Reference
URL	https://bugs.php.net/bug.php?id=71704
URL	https://cwe.mitre.org/data/definitions/20.html

PHP 'php_url_parse_ex' Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The php_url_parse_ex function in ext/standard/url.c in PHP before 5.5.38 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via vectors involving the smart_str data type.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6288
BUGTRAQ	http://www.securityfocus.com/bid/92111
URL	http://git.php.net/?p=php-src.git;a=commit;h=629e4da7cc8b174acdeab84969cbfc606a019b31
URL	http://php.net/ChangeLog-5.php
URL	https://support.apple.com/HT207170
URL	https://bugs.php.net/70480
URL	https://cwe.mitre.org/data/definitions/119.html

PHP php_zip.c 'getFromIndex', 'getFromName' Heap Overflow — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Multiple integer overflows in php_zip.c in the zip extension in PHP before 7.0.6 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted call to (1) getFromIndex or (2) getFromName in the ZipArchive class.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3078
URL	https://cwe.mitre.org/data/definitions/190.html
URL	https://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=71923
URL	https://github.com/php/php-src/commit/3b8d4de300854b3517c7acb239b84f7726c1353c?w=1
URL	https://security-tracker.debian.org/tracker/CVE-2016-3078

PHP php_zip.c Zip Extension Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

php_zip.c in the zip extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data containing a ZipArchive object.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5773
BUGTRAQ	http://www.securityfocus.com/bid/91397
URL	https://bugs.php.net/bug.php?id=72434
URL	http://github.com/php/php-src/commit/f6aef68089221c5ea047d4a74224ee3deead99a6?w=1
URL	http://php.net/ChangeLog-5.php
URL	https://support.apple.com/HT207170
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/416.html

PHP 'process_nested_data' Function Use-After-Free Flaw High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate numerical keys within the serialized properties of an object. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8142.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0231

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/72539
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1185397
URL	https://bugs.php.net/bug.php?id=68710
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://support.apple.com/HT205267
URL	https://github.com/php/php-src/commit/b585a3aed7880a5fa5c18e2b838fc96f40e075bd
URL	http://advisories.mageia.org/MGASA-2015-0040.html

PHP 'process_nested_data' Function Use-After-Free Remote Code Execution Flaw

High

Vulnerability Details

Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages use of the unset function within an __wakeup function, a related issue to CVE-2015-0231.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2787
BUGTRAQ	http://www.securityfocus.com/bid/73431

Type	Reference
URL	https://support.apple.com/HT205267
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	https://support.apple.com/kb/HT205031
URL	https://bugs.php.net/bug.php?id=68976
URL	https://gist.github.com/smalyshev/eea9eafc7c88a4a6d10d
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html

PHP sanitizing.c 'php_filter_encode' Integer Overflow Denial of Service

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Integer overflow in the php_filter_encode_url function in ext/filter/sanitizing_filters.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4345
URL	https://bugs.php.net/bug.php?id=71637
URL	http://php.net/ChangeLog-7.php

PHP 'sapi/fpm/fpm/fpm_unix.c' Privilege Escalation Vulnerability — High

Vulnerability Details

sapi/fpm/fpm/fpm_unix.c in the FastCGI Process Manager (FPM) in PHP before 5.4.28 and 5.5.x before 5.5.12 uses 0666 permissions for the UNIX socket, which allows local users to gain privileges via a crafted FastCGI client.
Impact:
An attacker could gain escalated privileges on the target system.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0185
URL	https://hoffmann-christian.info/files/php-fpm/0001-Fix-bug-67060-use-default-mode-of-660.patch
URL	http://www.php.net/archive/2014.php#id2014-05-01-1
URL	http://php.net/downloads.php
URL	https://bugs.launchpad.net/ubuntu/+source/php5/+bug/1307027
URL	https://bugs.php.net/bug.php?id=67060
URL	https://github.com/php/php-src/commit/35ceea928b12373a3b1e3eecdc32ed323223a40d
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1092815
URL	http://support.apple.com/kb/HT6443

PHP 'Serializable Interface, SplObjectStorage class, SplDoublyLinkedList class' Multiple Use-after-free Remote Code Execution — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Multiple use-after-free vulnerabilities in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 allow remote attackers to execute arbitrary code via vectors related to (1) the Serializable interface, (2) the SplObjectStorage class, and (3) the SplDoublyLinkedList class, which are mishandled during unserialization.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6834
BUGTRAQ	http://www.securityfocus.com/bid/76649
URL	https://bugs.php.net/bug.php?id=70172
URL	https://bugs.php.net/bug.php?id=70366
URL	https://bugs.php.net/bug.php?id=70365
URL	http://php.net/ChangeLog-5.php

PHP 'session.c' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6290
BUGTRAQ	http://www.securityfocus.com/bid/92097
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/72562
URL	https://support.apple.com/HT207170
URL	http://php.net/ChangeLog-7.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=3798eb6fd5dddb211b01d41495072fd9858d4e32
URL	https://cwe.mitre.org/data/definitions/416.html

PHP Session Deserializer 'php_var_unserialize' Remote Code Execution

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The session deserializer in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 mishandles multiple php_var_unserialize calls, which allow remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted session content.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6835
BUGTRAQ	http://www.securityfocus.com/bid/76734
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=70219

PHP 'simplestring_addn' Denial of Service Vulnerability High

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function.
Impact:
An attacker could cause a denial of service condition on the asset.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6296
BUGTRAQ	http://www.securityfocus.com/bid/92095
URL	http://git.php.net/?p=php-src.git;a=commit;h=e6c48213c22ed50b2b987b479fcc1ac709394caa
URL	http://php.net/ChangeLog-5.php
URL	https://support.apple.com/HT207170
URL	http://php.net/downloads.php
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/72606
URL	https://cwe.mitre.org/data/definitions/119.html

PHP 'snmp.c' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6295
BUGTRAQ	http://www.securityfocus.com/bid/92094
URL	https://cwe.mitre.org/data/definitions/416.html
URL	http://git.php.net/?p=php-src.git;a=commit;h=cab1c3b3708eead315e033359d07049b23b147a3
URL	https://bugs.php.net/72479
URL	https://support.apple.com/HT207170
URL	http://php.net/ChangeLog-5.php
URL	http://php.net/ChangeLog-7.php

PHP SoapClient Multiple Type Confusion Denial of Service Vulnerabilities

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The SoapClient implementation in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an unexpected data type, related to "type confusion" issues in the (1) SoapClient::__getLastRequest, (2) SoapClient::__getLastResponse, (3) SoapClient::__getLastRequestHeaders, (4) SoapClient::__getLastResponseHeaders, (5) SoapClient::__getCookies, and (6) SoapClient::__setCookie methods.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4600
BUGTRAQ	http://www.securityfocus.com/bid/74413
URL	https://bugs.php.net/bug.php?id=69152
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://php.net/ChangeLog-5.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=0c136a2abd49298b66acb0cad504f0f972f5bfe8

PHP soap.c 'SoapClient__call' Arbitrary Code Execution — High

Vulnerability Details

The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage headers, which allows remote attackers to execute arbitrary code via crafted serialized data that triggers a "type confusion" in the serialize_function_call function.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6836
BUGTRAQ	http://www.securityfocus.com/bid/76644
URL	https://bugs.php.net/bug.php?id=70388

PHP 'soap.c' Type Confusion Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The SoapFault::__toString method in ext/soap/soap.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information, cause a denial of service (application crash), or possibly execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4599
BUGTRAQ	http://www.securityfocus.com/bid/75251
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://php.net/ChangeLog-5.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=51856a76f87ecb24fe1385342be43610fb6c86e4
URL	https://bugs.php.net/bug.php?id=69152

PHP spl_array.c SplArray Unserialization Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7417
BUGTRAQ	http://www.securityfocus.com/bid/93007
URL	http://www.php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://github.com/php/php-src/commit/ecb7f58a069be0dec4a6131b6351a761f808f22e?w=1
URL	https://www.tenable.com/security/tns-2016-19
URL	https://bugs.php.net/bug.php?id=73029

PHP spl_array.c 'SPL Extension' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5771
BUGTRAQ	http://www.securityfocus.com/bid/91401
URL	http://github.com/php/php-src/commit/3f627e580acfdaf0595ae3b115b8bec677f203ee?w=1
URL	https://support.apple.com/HT207170
URL	https://bugs.php.net/bug.php?id=72433
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/416.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731

PHP SPL 'ArrayObject, SplObjectStorage, SplDoublyLinkedList' Multiple Use-after-free Remote Code Execution

High

Vulnerability Details

Multiple use-after-free vulnerabilities in SPL in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allow remote attackers to execute arbitrary code via vectors involving (1) ArrayObject, (2) SplObjectStorage, and (3) SplDoublyLinkedList, which are mishandled during unserialization.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6831
BUGTRAQ	http://www.securityfocus.com/bid/76737

Type	Reference
URL	https://bugs.php.net/bug.php?id=70155
URL	https://bugs.php.net/bug.php?id=70169
URL	https://bugs.php.net/bug.php?id=70166
URL	https://bugs.php.net/bug.php?id=70168

PHP SPL Component Type Confusion Vulnerability High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3515
BUGTRAQ	http://www.securityfocus.com/bid/68237
URL	https://bugs.php.net/bug.php?id=67492
URL	http://git.php.net/?p=php-src.git;a=commit;h=88223c5245e9b470e1e6362bfd96829562ffe6ab
URL	http://support.apple.com/kb/HT6443
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html

PHP spl_directory.c 'SplFileObject::fread' Denial of Service — High

Vulnerability Details

Integer overflow in the SplFileObject::fread function in spl_directory.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer argument, a related issue to CVE-2016-5096.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5770
BUGTRAQ	http://www.securityfocus.com/bid/91403
URL	http://github.com/php/php-src/commit/7245bff300d3fa8bacbef7897ff080a6f1c23eba?w=1
URL	https://bugs.php.net/bug.php?id=72262
URL	https://support.apple.com/HT207170
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	https://cwe.mitre.org/data/definitions/190.html
URL	http://php.net/ChangeLog-5.php

PHP spl_observer.c SplObjectStorage Unserialize Implementation Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c in PHP before 7.0.12 does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7480
BUGTRAQ	http://www.securityfocus.com/bid/95152
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://blog.checkpoint.com/2016/12/27/check-point-discovers-three-zero-day-vulnerabilities-web-programming-language-php-7
URL	http://blog.checkpoint.com/wp-content/uploads/2016/12/PHP_Technical_Report.pdf
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=73257
URL	https://github.com/php/php-src/commit/61cdd1255d5b9c8453be71aacbbf682796ac77d4

PHP 'spl_ptr_heap_insert' Function Arbitrary Code Execution Vulnerability

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in the spl_ptr_heap_insert function in ext/spl/spl_heap.c in PHP before 5.5.27 and 5.6.x before 5.6.11 allows remote attackers to execute arbitrary code by triggering a failed SplMinHeap::compare operation.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4116
URL	https://www.htbridge.com/advisory/HTB23262
URL	https://bugs.php.net/bug.php?id=69737
URL	http://php.net/ChangeLog-5.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=1cbd25ca15383394ffa9ee8601c5de4c0f2f90e1

PHP string.c 'str_pad' Denial of Service — High

Vulnerability Details

Integer overflow in the str_pad function in ext/standard/string.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long string, leading to a heap-based buffer overflow.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4346
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=71637

PHP 'tar.c' Stack Buffer Overflow — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Stack-based buffer overflow in ext/phar/tar.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TAR archive.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2554
URL	http://php.net/ChangeLog-5.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://bugs.php.net/bug.php?id=71488

PHP 'uncompressed_filesize' Crafted PHAR Archive Denial of Service Vulnerability

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to ext/phar/util.c and ext/phar/zip.c.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7414
BUGTRAQ	http://www.securityfocus.com/bid/93004
URL	https://www.tenable.com/security/tns-2016-19
URL	http://www.php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://github.com/php/php-src/commit/0bfb970f43acd1e81d11be1154805f86655f15d5?w=1
URL	https://bugs.php.net/bug.php?id=72928

PHP 'var_unserializer.c' Integer Overflow — High

Vulnerability Details

Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3669
BUGTRAQ	http://www.securityfocus.com/bid/70611

Type	Reference
URL	https://support.apple.com/HT204659
URL	http://linux.oracle.com/errata/ELSA-2014-1768.html
URL	http://linux.oracle.com/errata/ELSA-2014-1767.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1154500
URL	http://git.php.net/?p=php-src.git;a=commit;h=56754a7f9eba0e4f559b6ca081d9f2a447b3f159
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=68044

PHP var_unserializer.c Invalid Object Denial of Service Vulnerability High

Vulnerability Details

ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7124
BUGTRAQ	http://www.securityfocus.com/bid/92756
URL	https://bugs.php.net/bug.php?id=72663
URL	https://www.tenable.com/security/tns-2016-19

Type	Reference
URL	http://www.php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/502.html
URL	https://github.com/php/php-src/commit/20ce2fe8e3c211a42fee05a461a5881be9a8790e?w=1

PHP var_unserializer.re 'finish_nested_data' Buffer Overlow High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The finish_nested_data function in ext/standard/var_unserializer.re in PHP before 5.6.31, 7.0.x before 7.0.21, and 7.1.x before 7.1.7 is prone to a buffer over-read while unserializing untrusted data. Exploitation of this issue can have an unspecified impact on the integrity of PHP.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12933
BUGTRAQ	http://www.securityfocus.com/bid/99490
URL	https://bugs.php.net/bug.php?id=74111
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://php.net/ChangeLog-7.php
URL	http://php.net/ChangeLog-5.php

PHP var_unserializer.re Object Deserialization Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/standard/var_unserializer.re in PHP before 5.6.26 mishandles object-deserialization failures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an unserialize call that references a partially constructed object.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7411
BUGTRAQ	http://www.securityfocus.com/bid/93009
URL	https://github.com/php/php-src/commit/6a7cc8ff85827fa9ac715b3a83c2d9147f33cd43?w=1
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://bugs.php.net/bug.php?id=73052

PHP 'var_unserializer.re' Use-after-free Vulnerability — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.36, 5.5.x before 5.5.20, and 5.6.x before 5.6.4 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate keys within the serialized properties of an object, a different vulnerability than CVE-2004-1019.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8142
BUGTRAQ	http://www.securityfocus.com/bid/71791
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=68594
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1175718
URL	http://git.php.net/?p=php-src.git;a=commit;h=630f9c33c23639de85c3fd306b209b538b73b4c9
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html

PHP Wakeup Processing Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

PHP through 5.6.27 and 7.x through 7.0.12 mishandles property modification during __wakeup processing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data, as demonstrated by Exception::__toString with DateInterval::__wakeup.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9138
BUGTRAQ	http://www.securityfocus.com/bid/95268
URL	https://bugs.php.net/bug.php?id=73147

Type	Reference
URL	https://cwe.mitre.org/data/definitions/416.html

PHP wddx.c 'php_wddx_process_data' Denial of Service Vulnerability High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call that mishandles a dateTime element in a wddxPacket XML document.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7129
BUGTRAQ	http://www.securityfocus.com/bid/92758
URL	https://github.com/php/php-src/commit/426aeb2808955ee3d3f52e0cfb102834cdb836a5?w=1
URL	https://www.tenable.com/security/tns-2016-19
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=72749

PHP wddx.c 'php_wddx_process_data' Double Free Vulnerability High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Double free vulnerability in the php_wddx_process_data function in wddx.c in the WDDX extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted XML data that is mishandled in a wddx_deserialize call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5772
BUGTRAQ	http://www.securityfocus.com/bid/91398
URL	https://cwe.mitre.org/data/definitions/415.html
URL	https://support.apple.com/HT207170
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-7.php
URL	http://github.com/php/php-src/commit/a44c89e8af7c2410f4bfc5e097be2a5d0639a60c?w=1
URL	https://bugs.php.net/bug.php?id=72340
URL	http://php.net/ChangeLog-5.php

PHP wddx.c 'wddx_stack_destroy' Denial of Service Vulnerability High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in the wddx_stack_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to mishandling in a wddx_deserialize call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7413
BUGTRAQ	http://www.securityfocus.com/bid/93006
URL	https://bugs.php.net/bug.php?id=72860
URL	http://www.php.net/ChangeLog-7.php
URL	https://www.tenable.com/security/tns-2016-19
URL	https://cwe.mitre.org/data/definitions/416.html
URL	https://github.com/php/php-src/commit/b88393f08a558eec14964a55d3c680fe67407712?w=1

PHP 'wddx.c' XML Document Denial of Service High

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9935
BUGTRAQ	http://www.securityfocus.com/bid/94846

Type	Reference
URL	https://bugs.php.net/bug.php?id=73631
URL	https://cwe.mitre.org/data/definitions/125.html
URL	https://github.com/php/php-src/commit/66fd44209d5ffcb9b3d1bc1b9fd8e35b485040c0
URL	http://www.php.net/ChangeLog-7.php

PHP WDDX Extension Use-after-free Vulnerability

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in wddx.c in the WDDX extension in PHP before 5.5.33 and 5.6.x before 5.6.19 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact by triggering a wddx_deserialize call on XML data containing a crafted var element.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3141
BUGTRAQ	http://www.securityfocus.com/bid/84271
URL	https://bugs.php.net/bug.php?id=71587
URL	http://git.php.net/?p=php-src.git;a=commit;h=b1bd4119bcafab6f9a8f84d92cd65eec3afeface
URL	https://php.net/ChangeLog-5.php
URL	https://support.apple.com/HT206567
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference
URL	http://www.oracle.com/technetwork/topics/security/bulletinoct2016-3090566.html

PHP xml.c 'xml_parse_into_struct' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The xml_parse_into_struct function in ext/xml/xml.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted XML data in the second argument, leading to a parser level of zero.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4539
BUGTRAQ	http://www.securityfocus.com/bid/90174
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	http://php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://git.php.net/?p=php-src.git;a=commit;h=dccda88f27a084bcbbb30198ace12b4e7ae961cc
URL	https://bugs.php.net/bug.php?id=72099
URL	http://php.net/ChangeLog-5.php

Type	Reference
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731

PHP xml.c 'xml_utf8_encode' Integer Overflow Denial of Service — High

Vulnerability Details

Integer overflow in the xml_utf8_encode function in ext/xml/xml.c in PHP before 7.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long argument to the utf8_encode function, leading to a heap-based buffer overflow.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4344
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=71637

PHP Zend Engine 'zend_ts_hash_graceful_destroy' Function Denial of Service Flaw — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Double free vulnerability in the zend_ts_hash_graceful_destroy function in zend_ts_hash.c in the Zend Engine in PHP through 5.5.20 and 5.6.x through 5.6.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9425
BUGTRAQ	http://www.securityfocus.com/bid/71800
URL	https://bugs.php.net/bug.php?id=68676
URL	http://git.php.net/?p=php-src.git;a=commit;h=fbf3a6bc1abcc8a5b5226b0ad9464c37f11ddbd6
URL	https://support.apple.com/HT205267
URL	http://git.php.net/?p=php-src.git;a=commit;h=24125f0f26f3787c006e4a51611ba33ee3b841cb
URL	http://advisories.mageia.org/MGASA-2015-0040.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://git.php.net/?p=php-src.git;a=commit;h=2bcf69d073190e4f032d883f3416dea1b027a39e

PHP 'zend_exceptions.c' Type Confusion Remote Code Execution — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exception::getTraceAsString function in Zend/zend_exceptions.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to execute arbitrary code via an unexpected data type, related to a "type confusion" issue.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4603
BUGTRAQ	http://www.securityfocus.com/bid/75252
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=69152
URL	http://php.net/ChangeLog-5.php

PHP zend_string_extend in 'Zend/zend_string.h' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The zend_string_extend function in Zend/zend_string.h in PHP through 7.1.5 does not prevent changes to string objects that result in a negative length, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact by leveraging a script's use of .= with a long string.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8923
BUGTRAQ	http://www.securityfocus.com/bid/98518
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://bugs.php.net/bug.php?id=74577

PHP ZIP Extension "_zip_cdir_new" Function Integer Overflow High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Integer overflow in the _zip_cdir_new function in zip_dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2331
URL	http://git.php.net/?p=php-src.git;a=commit;h=ef8fc4b53d92fbfcd8ef1abbd6f2f5fe2c4a11e5
URL	https://support.apple.com/HT205267
URL	https://bugs.php.net/bug.php?id=69253
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://php.net/ChangeLog-5.php

Ruby 'Oniguruma-mod' and PHP fetch_token in 'mbstring' Denial of Service

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write or read occurs in next_state_val() during regular expression compilation. Octal numbers larger than 0xff are not handled correctly in fetch_token() and fetch_token_in_cc(). A malformed regular expression containing an octal number in the form of '\700' would produce an invalid code point value larger than 0xff in next_state_val(), resulting in an out-of-bounds write memory corruption.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9226
BUGTRAQ	http://www.securityfocus.com/bid/101244
URL	https://github.com/kkos/oniguruma/issues/55
URL	https://cwe.mitre.org/data/definitions/787.html
URL	https://github.com/kkos/oniguruma/commit/f015fbdd95f76438cd86366467bb2b39870dd7c6
URL	https://github.com/kkos/oniguruma/commit/b4bf968ad52afe14e60a2dc8a95d3555c543353a

Ruby 'Oniguruma-mod' and PHP 'mbstring' Denial of Service High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in match_at() during regular expression searching. A logical error involving order of validation and access in match_at() could result in an out-of-bounds read from a stack buffer.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9224
BUGTRAQ	http://www.securityfocus.com/bid/101244

Type	Reference
URL	https://github.com/kkos/oniguruma/commit/690313a061f7a4fa614ec5cc8368b4f2284e059b
URL	https://github.com/kkos/oniguruma/issues/57
URL	https://cwe.mitre.org/data/definitions/125.html

Ruby 'Oniguruma-mod' and PHP 'mbstring' forward_search_range Denial of Service — High

Vulnerability Details

An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in mbc_enc_len() during regular expression searching. Invalid handling of reg->dmin in forward_search_range() could result in an invalid pointer dereference, as an out-of-bounds read from a stack buffer.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9227
BUGTRAQ	http://www.securityfocus.com/bid/100538
URL	https://github.com/kkos/oniguruma/issues/58
URL	https://github.com/kkos/oniguruma/commit/9690d3ab1f9bcd2db8cbe1fe3ee4a5da606b8814
URL	https://cwe.mitre.org/data/definitions/125.html

Ruby 'Oniguruma-mod' and PHP 'mbstring' parse_char_class Denial of Service — High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write occurs in bitset_set_range() during regular expression compilation due to an uninitialized variable from an incorrect state transition. An incorrect state transition in parse_char_class() could create an execution path that leaves a critical local variable uninitialized until it's used as an index, resulting in an out-of-bounds write memory corruption.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9228
URL	https://cwe.mitre.org/data/definitions/787.html
URL	https://github.com/kkos/oniguruma/issues/60
URL	https://github.com/kkos/oniguruma/commit/3b63d12038c8d8fc278e81c942fa9bec7c704c8b

Ruby 'Oniguruma-mod' and PHP unicode_unfold_key in 'mbstring' Buffer Overflow

High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds write in onigenc_unicode_get_case_fold_codes_by_str() occurs during regular expression compilation. Code point 0xFFFFFFFF is not properly handled in unicode_unfold_key(). A malformed regular expression could result in 4 bytes being written off the end of a stack buffer of expand_case_fold_string() during the call to onigenc_unicode_get_case_fold_codes_by_str(), a typical stack buffer overflow.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9225
URL	https://github.com/kkos/oniguruma/commit/166a6c3999bf06b4de0ab4ce6b088a468cc4029f
URL	https://github.com/kkos/oniguruma/issues/56
URL	https://cwe.mitre.org/data/definitions/787.html

Samba '4.x before 4.7.3' Remote Code Execution Vulnerability High

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a crafted SMB1 request.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-14746
BUGTRAQ	http://www.securityfocus.com/bid/101907
URL	https://www.samba.org/samba/security/CVE-2017-14746.html
URL	https://www.synology.com/support/security/Synology_SA_17_72_Samba
URL	https://cwe.mitre.org/data/definitions/416.html
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03817en_us

Samba Remote Code Execution Vulnerability High

Solution Details

Please upgrade to the most current stable release of Samba, available at http://www.samba.org.
Workarounds:
Add the parameter:

nt pipe support = no

to the [global] section of your smb.conf and restart smbd. This
prevents clients from accessing any named pipe endpoints. Note this
can disable some expected functionality for Windows clients.

Vulnerability Details

Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7494
BUGTRAQ	http://www.securityfocus.com/bid/98636
URL	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7494
URL	https://cwe.mitre.org/data/definitions/94.html
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03759en_us
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbns03755en_us
URL	https://www.samba.org/samba/security/CVE-2017-7494.html
URL	https://security.netapp.com/advisory/ntap-20170524-0001/
URL	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7494
URL	https://www.samba.org/samba/history/security.html

Samba Security Advisory January 2022 — High

Solution Details

Please upgrade to the latest version.

Vulnerability Details

Samba vulnerabilities range from a race condition (CVE-2021-43566) to a privilege escalation vulnerability (CVE_2021-44142). The race condition and sensitive information vulnerability require SMB1 and/or share available by NFS.

CVE-2021-44142: Requires Samba versions with vfs_fruit configured which allows an out-of-bounds read/write. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.5

CVSS Vector: AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-43566
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-0336
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-44141
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-44142
URL	https://www.samba.org/samba/history/security.html

SNMP Writeable Communities — High

Solution Details

SNMP should be disabled if it is not required on this host. If SNMP is required, writeable community strings should have their permission changed to be read only. If SNMP is required and writeable community strings are necessary, these strings should be configured to be difficult for an attacker to guess. Below are some sample methods for changing SNMP community strings on common platforms.

Cisco routers:
In Enable mode, type:
'snmp-server community ' to add a specified community string.
'no snmp-server community ' to remove a specified community string.
'no snmp-server' to disable the SNMP server.

HP JetDirect:
The read-only community strings of 'public' and 'internal' cannot be changed. These strings are used by the JetAdmin software, and are hard coded into the firmware. Please contact HP directly to find out how to properly secure a HP Printer. It is possible to change the write community string by typing the following via a TELNET session:
set-cmnty-name: NewString

The only valid workaround for this vulnerability on a HP JetDirect printer is to disable SNMP using the following command via TELNET:
snmp-config: 0

Without SNMP, the Embedded WebServer will not function properly, so it is recommended that EWS be disabled using the following command via TELNET: ews-config: 0

SNMP can be disabled in more recent versions of the JetDirect firmware. If this command is not available, please upgrade the printer firmware to the latest available.

Canon imageRUNNER:
Manage the SNMP settings through the administration console by navigating through: "Settings / Registration" > "Preferences" > "Network" > "SNMP Settings"

Other systems:
Consult the system's documentation or contact the system's vendor for further assistance.
Caveats:
In certain hosts, default community strings with writeable permissions are required. Changing these strings to read-only could cause other services and devices to not function properly.

Vulnerability Details

Hosts running the SNMP service use community strings to authenticate. This host was found to have default communities that have writeable permissions. A writeable community string allows data in the MIB to be written and changed. An attacker can use this vulnerability to gain information about the host and its environment, as well as change the host's configuration.

Impact:
A writeable community string gives the user access to a variety of management tasks such as rerouting network traffic, enabling or disabling services, and executing commands. Attackers can use this to fully compromise this host and potentially compromise other hosts on the network.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0517

Type	Reference
URL	http://www.phrack.com/issues.html?issue=50&id=7#article
URL	http://www.securityfocus.com/bid/986/discuss

Unquoted Windows Service Path Vulnerability — High

Vulnerability Details

This host has one or more Windows services that use an unquoted string that contains spaces to specify the path to the image that the service uses. This creates the potential for an unprivileged local user to elevate their privileges to that which the service runs under by placing a rogue executable in a user-accessible path which causes the service to load this executable instead.

As an example, a path such as C:\Program Files\Symantec\bin\symsrv.exe when used to specify the service, creates a potential hijack location if a user places a file called "Program.exe" in the C:\. Because the path is unquoted, Windows will read the string up to the space and attempt to load a file from that path by appending an extension. Thus, it will instead load C:\Program.exe.
Impact:
A malicious local user who has limited privileges can abuse this vulnerability to gain elevated permissions and gain full control over this host. Permissions granted are relative to the account under which the affected service runs.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Make sure that any Windows service which has a path that contains a space in it is enclosed in quotations. This can be done manually by editing the service. Additionally, the vendor of the software product which creates this service should be contacted to inform them of this vulnerability.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
URL	https://isc.sans.edu/diary/Help+eliminate+unquoted+path+vulnerabilities/14464
URL	http://cwe.mitre.org/data/definitions/428.html

VMware Security Advisory: VMSA-2015-0007 — High

Solution Details

VMware has released a fix for this flaw which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5177
BUGTRAQ	http://www.securityfocus.com/bid/76635
URL	https://www.vmware.com/security/advisories/VMSA-2015-0007.html
URL	https://cwe.mitre.org/data/definitions/415.html
URL	http://sourceforge.net/p/openslp/mercurial/ci/2bc15d0494f886d9c4fe342d23bc160605aea51d/
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1251064

VMware Security Advisory: VMSA-2018-0026 High

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

CVSS Base Score: 8.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6974
BUGTRAQ	http://www.securityfocus.com/bid/105660
URL	https://cwe.mitre.org/data/definitions/125.html
URL	https://www.vmware.com/security/advisories/VMSA-2018-0026.html

VMware Security Advisory: VMSA-2019-0012 High

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5684
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5521
URL	http://www.vmware.com/security/advisories/VMSA-2019-0012.html
URL	https://support.lenovo.com/us/en/product_security/LEN-28096
URL	https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0779
URL	https://www.vmware.com/security/advisories/VMSA-2019-0012.html
URL	https://nvidia.custhelp.com/app/answers/detail/a_id/4841

VMware Security Advisory: VMSA-2019-0022 High

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5544
URL	http://www.vmware.com/security/advisories/VMSA-2019-0022.html
URL	https://www.vmware.com/security/advisories/VMSA-2019-0022.html

VMware Security Advisory: VMSA-2020-0023 High

Solution Details

VMware has released a fix for this flaw which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3994
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3993
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3992

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3982
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3995
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3981
URL	https://www.vmware.com/security/advisories/VMSA-2020-0023.html

VMware Security Advisory: VMSA-2020-0026 High

Solution Details

VMware has released a fix for this flaw which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.2

CVSS Vector: AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-4005
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-4004
URL	https://www.vmware.com/security/advisories/VMSA-2020-0026.html

VMware Security Advisory: VMSA-2021-0002 High

Solution Details

VMware has released a fix for this flaw which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21972
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21973
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21974
URL	https://www.vmware.com/security/advisories/VMSA-2021-0002.html

Web Server Directory Traversal High

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

Solution Details

Please ensure all user supplied input is sanitized before use as a path for file access. If this web application was provided by a third party vendor, please contact the vendor for specific remediation instructions.

Vulnerability Details

The remote host is running a web server, web service, or web application that contains a directory traversal vulnerability. A remote, unauthenticated attacker can leverage this vulnerability to retrieve arbitrary files and possibly execute arbitrary programs on the remote host, including those which reside outside of the web root.

This arbitrary access to files and programs can be accomplished by submitting an HTTP GET request for a URL which contains a variation of '../'. An example of the path which was used to retrieve an arbitrary file from the vulnerable system is included in the data section of this vulnerability.

CVSS Base Score: 7.8

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:N/A:N

Type	Reference
URL	https://cwe.mitre.org/data/definitions/22.html

Windows 10 End of Life High

Solution Details

Upgrade to a supported version of Windows 10.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This asset is running a version of Windows 10 that has reached end of life status. As such, newly discovered vulnerabilities will no longer be patched by the vendor.
Impact:
Even though vulnerabilities in this version of Windows 10 may exist, Microsoft will not patch them. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this asset or its data.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://support.microsoft.com/en-us/help/13853/windows-lifecycle-fact-sheet

Windows EFSRPC NTLM Relay Vulnerability (PetitPotam) High

Solution Details

Microsoft has provided a patch for this vulnerability. Additionally, there are other mitigation steps that can be taken that include disabling NTLM authentication and implementing RPC filters to block requests to the affected RPC interface.

Please refer to the external references section and specifically to the documentation provided by Microsoft on how to address this vulnerability.

Vulnerability Details

This asset is running a version of Windows that is susceptible to an NTLM relay attack via the EFSRPC interface. It is possible for an unauthenticated attacker to send a specially crafted RPC request to this interface and cause the target to connect to a malicious relay server which can then impersonate the target to authenticate against remote services.
Impact:
Exploitation of this vulnerability against a domain controller target can result in the complete compromise of the domain.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.3

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36942
URL	https://kb.cert.org/vuls/id/405600
URL	https://msrc.microsoft.com/update-guide/vulnerability/ADV210003
URL	https://github.com/topotam/PetitPotam

Zend NULL Pointer Denial of Service — High

Vulnerability Details

Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 does not validate certain Exception objects, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger unintended method execution via crafted serialized data.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8876
URL	https://bugs.php.net/bug.php?id=70121

Apache httpd Digest Authorization Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.4

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9788
BUGTRAQ	http://www.securityfocus.com/bid/99569
URL	https://httpd.apache.org/security/vulnerabilities_22.html
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03908en_us
URL	https://support.apple.com/HT208221
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://security.netapp.com/advisory/ntap-20170911-0002/

Apache HTTP 'HTTP/2 mod' Denial of Service Vulnerability — Medium

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

Vulnerability Details

When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools.
Impact:
An attacker can exploit this vulnerability to cause a denial-of-service condition, denying service to legitimate users.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11993
URL	https://httpd.apache.org/download.cgi

Apache HTTP "RequestHeader unset" Directive Bypass Vulnerability Medium

Vulnerability Details

HTTP trailers could be used to replace HTTP headers late during request processing, potentially undoing or otherwise confusing modules that examined or modified request headers earlier.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to version 2.4.12 or later.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-5704
BUGTRAQ	http://www.securityfocus.com/bid/66550
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html
URL	http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
URL	https://support.apple.com/HT204659
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=1610674&r2=1610814&diff_format=h

Type	Reference
URL	http://martin.swende.se/blog/HTTPChunked.html
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://support.apple.com/HT205219
URL	http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html

Apache HTTP Server 'ap_some_auth_required' Function Remote Access Restrictions Bypass Vulnerability

Medium

Vulnerability Details

The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3185
BUGTRAQ	http://www.securityfocus.com/bid/75965
URL	http://httpd.apache.org/security/vulnerabilities_24.html
URL	http://www.apache.org/dist/httpd/CHANGES_2.4
URL	https://support.apple.com/HT205219

Type	Reference
URL	https://support.apple.com/kb/HT205031
URL	https://support.apple.com/HT205217
URL	https://github.com/apache/httpd/commit/cd2b7a26c776b0754fb98426a67804fd48118708

Apache HTTP Server 'Cache-Digest' Denial of Service Vulnerability — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.
Workarounds:
Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.

Vulnerability Details

A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards.
Impact:
An attacker can exploit this vulnerability to cause a denial-of-service condition, denying service to legitimate users.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-9490
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server 'cache_merge_headers_out' Function Denial of Service Vulnerability — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to version 2.4.12 or later.

Vulnerability Details

A NULL pointer deference was found in mod_cache. A malicious HTTP server could cause a crash in a caching forward proxy configuration. This crash would only be a denial of service if using a threaded MPM.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3581
BUGTRAQ	http://www.securityfocus.com/bid/71656
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://support.apple.com/kb/HT205031
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1149709
URL	http://svn.apache.org/viewvc/httpd/httpd/branches/2.4.x/CHANGES?view=markup&pathrev=1627749
URL	http://svn.apache.org/viewvc?view=revision&revision=1624234
URL	https://cwe.mitre.org/data/definitions/399.html
URL	https://support.apple.com/HT205219
URL	http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html

Apache HTTP Server Crafted Request Denial of Service Vulnerability — Medium

Vulnerability Details

By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service.
Impact:
An attacker could cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to External References for a link to download and update to the most recent stable version of Apache HTTP Server.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1333
URL	https://httpd.apache.org/download.cgi
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03909en_us
URL	https://cwe.mitre.org/data/definitions/399.html
URL	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2018-1333
URL	https://security.netapp.com/advisory/ntap-20180926-0007/

Apache HTTP Server 'deflate_in_filter' Function Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0118
BUGTRAQ	http://www.securityfocus.com/bid/68745
URL	http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES

Type	Reference
URL	https://support.apple.com/HT204659
URL	http://advisories.mageia.org/MGASA-2014-0305.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1120601
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/filters/mod_deflate.c?r1=1604353&r2=1610501&diff_format=h
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/filters/mod_deflate.c
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html
URL	http://httpd.apache.org/security/vulnerabilities_24.html
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://advisories.mageia.org/MGASA-2014-0304.html
URL	https://puppet.com/security/cve/cve-2014-0118

Apache HTTP Server Digest Authentication Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2161

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/95076
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.apple.com/HT208221
URL	https://security.netapp.com/advisory/ntap-20180423-0001/
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03725en_us
URL	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-2161
URL	https://www.tenable.com/security/tns-2017-04

Apache HTTP Server HTTP/2 Connections Crafted Request Denial of Service Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1333
URL	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2018-1333
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03909en_us
URL	https://cwe.mitre.org/data/definitions/399.html

Type	Reference
URL	https://security.netapp.com/advisory/ntap-20180926-0007/

Apache HTTP Server HTTP Chunked Request Smuggling Attack — Medium

Solution Details

Upgrade to version 2.2.31 or 2.4.16 or later.

Vulnerability Details

An HTTP request smuggling attack was possible due to a bug in parsing of chunked requests. A malicious client could force the server to misinterpret the request length, allowing cache poisoning or credential hijacking if an intermediary proxy is in use.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3183
BUGTRAQ	http://www.securityfocus.com/bid/75963
BUGTRAQ	http://www.securityfocus.com/bid/91787
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04926789
URL	http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html
URL	https://puppet.com/security/cve/CVE-2015-3183
URL	https://support.apple.com/HT205219
URL	http://httpd.apache.org/security/vulnerabilities_24.html
URL	http://www.apache.org/dist/httpd/CHANGES_2.4
URL	https://github.com/apache/httpd/commit/e427c41257957b57036d5a549b260b6185d1dd73
URL	http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html

Type	Reference
URL	http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
URL	https://support.apple.com/kb/HT205031
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html

Apache HTTP Server 'httpd' URL Normalization Inconsistency Vulnerability	Medium

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
Impact:
An attacker can leverage this issue to perform unauthorized actions in the context of the asset.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0220
BUGTRAQ	http://www.securityfocus.com/bid/107670
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://security.netapp.com/advisory/ntap-20190625-0007/
URL	https://httpd.apache.org/download.cgi
URL	https://cwe.mitre.org/data/definitions/399.html
URL	https://support.f5.com/csp/article/K44591505

Apache HTTP Server HTTP_PROXY Environment Variable Vulnerability

Medium

Vulnerability Details

HTTP_PROXY is a well-defined environment variable in a CGI process, which collided with a number of libraries which failed to avoid colliding with this CGI namespace. A mitigation is provided for the httpd CGI environment to avoid populating the "HTTP_PROXY" variable from a "Proxy:" header, which has never been registered by IANA.

This workaround and patch are documented in the ASF Advisory at asf-httpoxy-response.txt and incorporated in the 2.4.25 and 2.2.32 releases.

Note: This is not assigned an httpd severity, as it is a defect in other software which overloaded well-established CGI environment variables, and does not reflect an error in HTTP server software.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to version 2.2.32 or 2.4.45 or later.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5387
BUGTRAQ	http://www.securityfocus.com/bid/91816
URL	http://www.oracle.com/technetwork/topics/security/bulletinoct2016-3090566.html
URL	https://www.tenable.com/security/tns-2017-04
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://support.apple.com/HT208221
URL	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722

Type	Reference
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://www.apache.org/security/asf-httpoxy-response.txt
URL	https://httpoxy.org/
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03770en_us

Apache HTTP Server 'lua_websocket_read' Function Denial of Service Vulnerability

Medium

Vulnerability Details

A stack recursion crash in the mod_lua module was found. A Lua script executing the r:wsupgrade() function could crash the process if a malicious client sent a carefully crafted PING request.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to version 2.4.16 or later.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0228
BUGTRAQ	http://www.securityfocus.com/bid/73041
BUGTRAQ	http://www.securityfocus.com/bid/91787
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://github.com/apache/httpd/commit/643f0fcf3b8ab09a68f0ecd2aa37aafeda3e63ef
URL	http://svn.apache.org/repos/asf/httpd/httpd/branches/2.4.x/CHANGES
URL	http://advisories.mageia.org/MGASA-2015-0099.html

Type	Reference
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://support.apple.com/kb/HT205031
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
URL	https://support.apple.com/HT205219

Apache HTTP Server 'mod_auth_digest' Access Control Bypass Vulnerability	Medium

Vulnerability Details

In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
Impact:
An attacker could exploit this vulnerability to access the target asset in the context of another user, allowing them to perform unauthorized actions from that account, possibly aiding in further attacks.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6

CVSS Vector: AV:N/AC:M/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0217
BUGTRAQ	http://www.securityfocus.com/bid/107668
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1695020
URL	https://security.netapp.com/advisory/ntap-20190423-0001/
URL	https://cwe.mitre.org/data/definitions/362.html

Type	Reference
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server 'mod_cache_socache' Out of Bound Read Denial of Service Vulnerability

Medium

Solution Details

Upgrade to version 2.4.33 or later.

Vulnerability Details

A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.33 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1303
BUGTRAQ	http://www.securityfocus.com/bid/103522
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://security.netapp.com/advisory/ntap-20180601-0004/
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03909en_us
URL	https://cwe.mitre.org/data/definitions/125.html

Apache HTTP Server 'mod_cgid' Module Denial of Service

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0231
BUGTRAQ	http://www.securityfocus.com/bid/68742
URL	http://httpd.apache.org/security/vulnerabilities_24.html
URL	http://advisories.mageia.org/MGASA-2014-0304.html
URL	http://advisories.mageia.org/MGASA-2014-0305.html
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_cgid.c?r1=1482522&r2=1535125&diff_format=h
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	http://packetstormsecurity.com/files/130769/RSA-Digital-Certificate-Solution-XSS-Denial-Of-Service.html
URL	https://support.apple.com/HT204659
URL	https://puppet.com/security/cve/cve-2014-0231
URL	http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_cgid.c
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_cgid.c?r1=1565711&r2=1610509&diff_format=h
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1120596

Apache HTTP Server 'mod_dav' Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-6438
BUGTRAQ	http://www.securityfocus.com/bid/66303
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	http://www.vmware.com/security/advisories/VMSA-2014-0012.html
URL	https://support.apple.com/HT204659
URL	https://puppet.com/security/cve/cve-2013-6438
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/util.c?r1=1528718&r2=1556428&diff_format=h
URL	http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	https://support.apple.com/kb/HT6535
URL	https://blogs.oracle.com/sunsecurity/entry/multiple_input_validation_vulnerabilities_in1
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676091

Type	Reference
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/dav/main/util.c
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21669554
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698
URL	http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
URL	http://advisories.mageia.org/MGASA-2014-0135.html
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676092
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html

Apache HTTP Server 'mod_http2' Memory Corruption Vulnerability — Medium

Vulnerability Details

HTTP/2 very early pushes, for example configured with "H2PushResource", could lead to an overwrite of memory in the pushing request's pool, leading to crashes. The memory copied is that of the configured push link header values, not data supplied by the client.
Impact:
An attacker can exploit this vulnerability to cause a denial-of-service condition, denying service to legitimate users.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-10081
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server 'mod_http2' Module Denial of Service Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The mod_http2 module in the Apache HTTP Server 2.4.17 through 2.4.23, when the Protocols configuration includes h2 or h2c, does not restrict request-header length, which allows remote attackers to cause a denial of service (memory consumption) via crafted CONTINUATION frames in an HTTP/2 request.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-8740
BUGTRAQ	http://www.securityfocus.com/bid/94650
URL	https://security.netapp.com/advisory/ntap-20180423-0001/
URL	https://www.tenable.com/security/tns-2017-04
URL	https://support.apple.com/HT208221
URL	https://github.com/apache/httpd/commit/29c63b786ae028d82405421585e91283c8fa0da3
URL	http://packetstormsecurity.com/files/140023/Apache-HTTPD-Web-Server-2.4.23-Memory-Exhaustion.html
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03725en_us

Apache HTTP Server 'mod_http2' Read-After-Free (CVE-2019-0196) — Medium

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

Vulnerability Details

Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparision when determining the method of a request and thus process the request incorrectly.
Impact:
An attacker could exploit this vulnerability and get more information about the targeted asset, possibly aiding in further attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0196
BUGTRAQ	http://www.securityfocus.com/bid/107669
URL	https://support.f5.com/csp/article/K44591505
URL	https://cwe.mitre.org/data/definitions/416.html
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://httpd.apache.org/download.cgi
URL	https://security.netapp.com/advisory/ntap-20190617-0002/
URL	http://www.apache.org/dist/httpd/CHANGES_2.4.39

Apache HTTP Server 'mod_http2' Read-After-Free (CVE-2019-10082) Medium

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

Vulnerability Details

Using fuzzed network input, the http/2 session handling could be made to read memory after being freed, during connection shutdown.
Impact:
An attacker can exploit this vulnerability to cause a denial-of-service condition, denying service to legitimate users.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.4

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-10082
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server ' mod_log_config' Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0098
BUGTRAQ	http://www.securityfocus.com/bid/66303
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10698
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676092
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676091
URL	https://support.apple.com/HT204659
URL	https://httpd.apache.org/security/vulnerabilities_24.html

Type	Reference
URL	http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
URL	http://www.vmware.com/security/advisories/VMSA-2014-0012.html
URL	https://blogs.oracle.com/sunsecurity/entry/multiple_input_validation_vulnerabilities_in1
URL	https://support.apple.com/kb/HT6535
URL	http://advisories.mageia.org/MGASA-2014-0135.html
URL	http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/loggers/mod_log_config.c?r1=1575394&r2=1575400&diff_format=h
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/loggers/mod_log_config.c
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21668973
URL	http://support.f5.com/kb/en-us/solutions/public/15000/300/sol15320.html
URL	https://puppet.com/security/cve/cve-2014-0098
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html

Apache HTTP Server 'mod_lua' Access Restriction Bypass Vulnerability

Medium

Vulnerability Details

mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-8109
BUGTRAQ	http://www.securityfocus.com/bid/73040
URL	https://issues.apache.org/bugzilla/show_bug.cgi?id=57204
URL	https://github.com/apache/httpd/commit/3f1693d558d0758f829c8b53993f1749ddf6ffcb
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1174077
URL	http://advisories.mageia.org/MGASA-2015-0011.html
URL	https://support.apple.com/HT205219
URL	https://support.apple.com/kb/HT205031
URL	http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html

Apache HTTP Server 'mod_proxy' Cross-Site Scripting Vulnerability — Medium

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

Vulnerability Details

A limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.
Impact:
An attacker could leverage this vulnerability to redirect users to a page of the attacker's choice which could lead to a disclosure of sensitive information.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-10092
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server 'mod_proxy' Module Denial of Service — Medium

Vulnerability Details

The mod_proxy module in the Apache HTTP Server 2.4.x before 2.4.10, when a reverse proxy is enabled, allows remote attackers to cause a denial of service (child-process crash) via a crafted HTTP Connection header.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0117
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c?r1=1599486&r2=1610674&diff_format=h
URL	http://httpd.apache.org/security/vulnerabilities_24.html
URL	https://support.apple.com/HT204659
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1120599
URL	http://zerodayinitiative.com/advisories/ZDI-14-239/
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/proxy_util.c?r1=1609680&r2=1610674&diff_format=h

Type	Reference
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/proxy_util.c
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/proxy/mod_proxy_http.c
URL	http://advisories.mageia.org/MGASA-2014-0305.html

Apache HTTP Server 'mod_rewrite' Redirect Vulnerability — Medium

Vulnerability Details

Redirects configured with 'mod_rewrite' that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
Impact:
Exploiting these issues will allow an attacker to bypass security restrictions or construct a crafted URI and enticing a user to follow it. When an unsuspecting victim follows the link, they may be redirected to an attacker-controlled site; this may aid in phishing attacks.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-1927
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server 'mod_session_cookie' Expiry Time Ignored Vulnerability — Medium

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

Vulnerability Details

In Apache HTTP Server 2.4 release 2.4.37 and prior, mod_session checks the session expiry time before decoding the session. This causes session expiry time to be ignored for mod_session_cookie sessions since the expiry time is loaded when the session is decoded.
Impact:
An attacker can leverage this issue to perform unauthorized actions. This may aid in further attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-17199
BUGTRAQ	http://www.securityfocus.com/bid/106742
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
URL	https://httpd.apache.org/download.cgi
URL	https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html
URL	https://cwe.mitre.org/data/definitions/384.html
URL	https://security.netapp.com/advisory/ntap-20190125-0001/

Apache HTTP Server 'mod_status' Module Race Condition — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0226
BUGTRAQ	http://www.securityfocus.com/bid/68678
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_status.c
URL	http://advisories.mageia.org/MGASA-2014-0305.html
URL	http://svn.apache.org/repos/asf/httpd/httpd/branches/2.2.x/CHANGES
URL	https://support.apple.com/HT204659
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	https://puppet.com/security/cve/cve-2014-0226
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/generators/mod_status.c?r1=1450998&r2=1610491&diff_format=h
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/lua/lua_request.c
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/modules/lua/lua_request.c?r1=1588989&r2=1610491&diff_format=h
URL	http://zerodayinitiative.com/advisories/ZDI-14-236/
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1120603
URL	http://httpd.apache.org/security/vulnerabilities_24.html
URL	http://advisories.mageia.org/MGASA-2014-0304.html
URL	https://cwe.mitre.org/data/definitions/362.html

Apache HTTP Server 'mod_userdir' CRLF Injection Vulnerability — Medium

Vulnerability Details

Possible CRLF injection allowing HTTP response splitting attacks for sites which use mod_userdir. This issue was mitigated by changes made in 2.4.25 and 2.2.32 which prohibit CR or LF injection into the "Location" or other outbound header key or value. Fixed in Apache HTTP Server 2.4.25 (Affected 2.4.1-2.4.23). Fixed in Apache HTTP Server 2.2.32 (Affected 2.2.0-2.2.31).
Impact:
Attackers can leverage this issue to influence or misrepresent how web content is served, cached, or interpreted. This could aid in various attacks that try to entice client users into having a false sense of trust.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most current version of Apache HTTP Server.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4975
BUGTRAQ	http://www.securityfocus.com/bid/105093
URL	https://httpd.apache.org/security/vulnerabilities_22.html#CVE-2016-4975
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03908en_us
URL	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-4975
URL	https://security.netapp.com/advisory/ntap-20180926-0006/
URL	https://cwe.mitre.org/data/definitions/93.html
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server Multiple Vulnerabilities — Medium

Vulnerability Details

CVE-2017-15710
mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials.
If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A

header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

CVE-2017-15715
The expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename.
This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

CVE-2018-1283
When mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header.
This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.

CVE-2018-1301
A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.33, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.

CVE-2018-1302
When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.33 could have written a NULL pointer potentially to an already freed memory.
The memory pools maintained by the server make this vulnerabilty hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

CVE-2018-1303
A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.33 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache.

CVE-2018-1312
When generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed.
In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.

Solution Details

Upgrade to version 2.4.33 or later.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1301
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1312
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15715
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1283
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15710
BUGTRAQ	http://www.securityfocus.com/bid/103515
BUGTRAQ	http://www.securityfocus.com/bid/103520
BUGTRAQ	http://www.securityfocus.com/bid/103525
BUGTRAQ	http://www.securityfocus.com/bid/103524
BUGTRAQ	http://www.securityfocus.com/bid/103512
URL	https://cwe.mitre.org/data/definitions/787.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03909en_us
URL	https://security.netapp.com/advisory/ntap-20180601-0004/

Apache HTTP Server Padding Oracle Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0736
BUGTRAQ	http://www.securityfocus.com/bid/95078
URL	https://support.apple.com/HT208221
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03725en_us
URL	https://cwe.mitre.org/data/definitions/310.html
URL	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-0736
URL	https://www.tenable.com/security/tns-2017-04
URL	https://security.netapp.com/advisory/ntap-20180423-0001/

Apache HTTP Server Response Splitting Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-8743
BUGTRAQ	http://www.securityfocus.com/bid/95077
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://security.netapp.com/advisory/ntap-20180423-0001/
URL	https://www.tenable.com/security/tns-2017-04
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03725en_us
URL	https://support.apple.com/HT208221
URL	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2016-8743
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbmu03753en_us

Apache HTTP Server Security Update 2.4.49 — Medium

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

Vulnerability Details

Apache HTTP Server's mod_proxy_wstunnel, mod_proxy_http, and mod_auth_digest have vulnerabilities that can range from Denial-of-Service to Stack/cache poisoning.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-34798
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-33193
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-40438

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-39275
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36160
URL	https://httpd.apache.org/download.cgi
URL	https://httpd.apache.org/security/vulnerabilities_24.html

Apache HTTP Server 'SETTINGS' Denial of Service Vulnerability — Medium

Vulnerability Details

In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
Impact:
An attacker could cause a denial of service condition on the asset.

Solution Details

Refer to External References for a link to download and update to the most recent stable version of Apache HTTP Server.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-11763
BUGTRAQ	http://www.securityfocus.com/bid/105414
URL	https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://httpd.apache.org/download.cgi

Type	Reference
URL	https://security.netapp.com/advisory/ntap-20190204-0004/
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03909en_us

Apache HTTP Server Slow Request Bodies Denial of Service Vulnerability

Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

By sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 connections.
Impact:
Attackers may leverage this issue to cause a denial-of-service condition, denying service to legitimate users.

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-17189
BUGTRAQ	http://www.securityfocus.com/bid/106685
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
URL	https://cwe.mitre.org/data/definitions/400.html
URL	https://security.netapp.com/advisory/ntap-20190125-0001/
URL	https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html

Type	Reference
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server URL Redirect Vulnerability — Medium

Vulnerability Details

Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
Impact:
An attacker could leverage this vulnerability to redirect users to a page of the attacker's choice which could lead to a disclosure of sensitive information.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Apache HTTP Server.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-10098
URL	https://httpd.apache.org/download.cgi

Apache HTTP Server winnt_accept Function Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Memory leak in the winnt_accept function in server/mpm/winnt/child.c in the WinNT MPM in the Apache HTTP Server 2.4.x before 2.4.10 on Windows, when the default AcceptFilter is enabled, allows remote attackers to cause a denial of service (memory consumption) via crafted requests.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3523
BUGTRAQ	http://www.securityfocus.com/bid/68747
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/server/mpm/winnt/child.c
URL	http://svn.apache.org/viewvc/httpd/httpd/trunk/server/mpm/winnt/child.c?r1=1608785&r2=1610652&diff_format=h
URL	http://httpd.apache.org/security/vulnerabilities_24.html

Apache 'Optionsbleed' UAF Memory Leak — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Apply the patch provided by the vendor
Workarounds:
This bug is produced when the Limit directive in an .htaccess file is misused, as below, by specifying a bogus header value:

```
"
<Limit bogusheader>
</Limit>
"
```

If applying the provided patch is not feasible, please ensure that all Limit directives used within .htaccess files are validated.

Vulnerability Details

CVE-2017-9798, 'Optionbleed', is a use after free error in the Apache web server that causes a corrupted Allow header to be returned in response to OPTIONS requests. Due to the nature of this vulnerability, exploitation is not deterministic, and requires multiple requests in order to attempt to determine if the vulnerability is present or not.
Impact:
A remote, unauthenticated attacker could leverage this vulnerability to obtain arbitrary pieces of

memory from the affected asset. The memory leaked changes over time with multiple requests, potentially allowing an attacker to gather a large amount of information, possibly including sensitive data.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9798
BUGTRAQ	http://www.securityfocus.com/bid/100872
BUGTRAQ	http://www.securityfocus.com/bid/105598
URL	https://cwe.mitre.org/data/definitions/416.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
URL	https://blog.fuzzing-project.org/60-Optionsbleed-HTTP-OPTIONS-method-can-leak-Apaches-server-memory.html
URL	https://blog.fuzzing-project.org/uploads/apache-2.2-optionsbleed-backport.patch
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
URL	https://github.com/apache/httpd/commit/29afdd2550b3d30a8defece2b95ae81edcf66ac9
URL	https://github.com/hannob/optionsbleed
URL	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
URL	https://svn.apache.org/viewvc/httpd/httpd/branches/2.4.x/server/core.c?r1=1805223&r2=1807754&pathrev=1807754&view=patch
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03909en_us
URL	https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2017-9798
URL	https://support.apple.com/HT208331
URL	https://security-tracker.debian.org/tracker/CVE-2017-9798
URL	https://security.netapp.com/advisory/ntap-20180601-0003/

Type	Reference
URL	http://openwall.com/lists/oss-security/2017/09/18/2
URL	https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html

Heimdal Man-in-the-Middle Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Heimdal before 7.4 allows remote attackers to impersonate services with Orpheus' Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unencrypted version provides an opportunity for successful server impersonation and other attacks. NOTE: this CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11103
BUGTRAQ	http://www.securityfocus.com/bid/99551
URL	https://www.orpheus-lyre.info/
URL	https://github.com/heimdal/heimdal/releases/tag/heimdal-7.4.0
URL	https://www.freebsd.org/security/advisories/FreeBSD-SA-17:05.heimdal.asc

Type	Reference
URL	https://www.samba.org/samba/security/CVE-2017-11103.html
URL	http://www.h5l.org/advisories.html?show=2017-07-11
URL	https://cwe.mitre.org/data/definitions/345.html
URL	https://support.apple.com/HT208144
URL	https://support.apple.com/HT208112
URL	https://support.apple.com/HT208221

Java Debugging Port Accessible — Medium

Solution Details

Remote debugging is not typically a necessary service. If remote debugging is not being performed, then consider disabling the debugging server. If the debugging server is necessary, restrict the IP addresses from which connections to the debugging service are accepted.

Vulnerability Details

The remote host is running a Java debugging server that is accessible via the network. A remote unauthenticated attacker can use this service to view, modify, and control execution of programs in the memory space of the exposed Java Virtual Machine (JVM) environment. Impact includes the possibility of denial of service as well as the disclosure of sensitive information that is available through the accessible memory space, such as passwords.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
URL	http://download.oracle.com/javaee/5/tutorial/doc/bnadl.html
URL	http://download.oracle.com/javase/1,5.0/docs/guide/jpda/jdwp-spec.html
URL	http://download.oracle.com/javase/1,5.0/docs/guide/jpda/jdwp/jdwp-protocol.html
URL	http://www.ibm.com/developerworks/opensource/library/os-eclipse-javadebug/index.html

jQuery Ajax Cross-Site Scripting Vulnerability

Medium

Solution Details

Upgrade to version 3.0.0 or later. Downloads available at the following link:

https://jquery.com/download/

Vulnerability Details

jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-9251
BUGTRAQ	http://www.securityfocus.com/bid/105658
URL	https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
URL	https://github.com/jquery/jquery/issues/2432
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://github.com/jquery/jquery/pull/2588
URL	https://ics-cert.us-cert.gov/advisories/ICSA-18-212-04
URL	https://snyk.io/vuln/npm:jquery:20150627
URL	https://github.com/jquery/jquery/pull/2588/commits/c254d308a7d3f1eac4d0b42837804cfffcba4bb2
URL	http://packetstormsecurity.com/files/152787/dotCMS-5.1.1-Vulnerable-Dependencies.html
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
URL	http://packetstormsecurity.com/files/153237/RetireJS-CORS-Issue-Script-Execution.html

Type	Reference
URL	https://github.com/jquery/jquery/commit/f60729f3903d17917dc351f3ac87794de379b0cc
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
URL	https://sw.aveva.com/hubfs/assets-2018/pdf/security-bulletin/SecurityBulletin_LFSec126.pdf

jQuery Cross-Site Scripting Vulnerability — Medium

Solution Details

Upgrade to version 3.5.0 or later. Downloads available at the following link:

https://jquery.com/download/

Vulnerability Details

In jQuery library, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.

Impact:
An attacker may leverage this issue to execute arbitrary HTML and script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker obtain information that could aid in launching further attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11023

jQuery Cross-Site Scripting Vulnerability — Medium

Vulnerability Details

In jQuery library, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code.
Impact:

An attacker may leverage this issue to execute arbitrary HTML and script code in the browser of an unsuspecting user in the context of the affected site. This may let the attacker obtain information that could aid in launching further attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to version 3.5.0 or later. Downloads available at the following link:

https://jquery.com/download/

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-11022

LDAP Channel Binding Vulnerability — Medium

Solution Details

Refer to the external links section for a detailed explanation of how to modify the registry in order to change this setting, which should be enabled by default after the March 2020 rollup is applied.

Registry setting for Active Directory Domain Services (AD DS) domain controllers mitigation:
key => HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters
value type => DWORD
value name => LdapEnforceChannelBinding
value data => 2

Vulnerability Details

A set of unsafe default configurations for LDAP channel binding exist on Active Directory Domain Controllers which permit LDAP clients to communicate without enforcing LDAP channel binding.
Impact:
Active Directory Domain Controllers could potentially be susceptible to an Elevation of Privilege attack.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.7

CVSS Vector: AV:A/AC:L/Au:S/C:N/I:P/A:N

Type	Reference
URL	https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirem
URL	https://support.microsoft.com/en-us/help/4034879/how-to-add-the-ldapenforcechannelbinding-registry-e
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023

LDAP Signing Vulnerability — Medium

Solution Details

Refer to the external links section for a detailed explanation of how to set specific GPO settings or modify the registry in order to change this setting, which should be enabled by default after the March 2020 rollup is applied.

To make changes via Group Policy Settings:
1. Set Server signing requirement:
a. Goto the Domain Controller Policy you wish to modify and edit via Group Policy Mgmt.
b. Goto Computer Configuration>Policies>Windows Settings>Security Settings>Local Policies>Security Options
c. Set Domain controller: LDAP server signing requirements to require signing

2. Set Client signing requirement:
a. Goto the Domain Policy you wish to modify and edit via Group Policy Mgmt.
b. Goto Computer Configuration>Policies>Windows Settings>Security Settings>Local Policies>Security Options
c. Set Network security: LDAP client signing requirements to require signing

Vulnerability Details

A set of unsafe default configurations for LDAP signing exist on Active Directory Domain Controllers which permit LDAP clients to communicate without enforcing LDAP signing.
Impact:
Active Directory Domain Controllers could potentially be susceptible to an Elevation of Privilege attack.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.7

CVSS Vector: AV:A/AC:L/Au:S/C:N/I:P/A:N

Type	Reference

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190023
URL	https://support.microsoft.com/en-us/help/935834/how-to-enable-ldap-signing-in-windows-server-2008

libxml 'libxml_disable_entity_loader' XXE and XEE Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/libxml/libxml.c in PHP before 5.5.22 and 5.6.x before 5.6.6, when PHP-FPM is used, does not isolate each thread from libxml_disable_entity_loader changes in other threads, which allows remote attackers to conduct XML External Entity (XXE) and XML Entity Expansion (XEE) attacks via a crafted XML document, a related issue to CVE-2015-5161.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.6

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8866
BUGTRAQ	http://www.securityfocus.com/bid/87470
URL	https://bugs.php.net/bug.php?id=64938
URL	https://bugs.launchpad.net/ubuntu/+source/php5/+bug/1509817
URL	http://git.php.net/?p=php-src.git;a=commit;h=de31324c221c1791b26350ba106cc26bad23ace9

MS09-001 SMB Remote Code Execution (Network Check) — Medium

Solution Details

Microsoft released Security Bulletin MS09-001 to address these issues. Please obtain and apply the appropriate Microsoft updates as described at

http://www.microsoft.com/technet/security/Bulletin/MS09-001.mspx.
A workaround is to block TCP ports 139 and 445 at the firewall, although multiple Windows services using these ports may not function.

Vulnerability Details

This host is running a version of Microsoft Windows which is vulnerable to a remote command execution flaw within the Server service. Remote attackers can leverage a NT Trans2 request with crafted SMB packets using malformed field values to execute arbitrary commands with user privileges. Unauthenticated attackers can also leverage the Server service with crafted SMB packets to gain control of this host or cause a denial of service.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4834
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4114
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2008-4835
BUGTRAQ	http://www.securityfocus.com/bid/31179
BUGTRAQ	http://www.securityfocus.com/bid/33121
BUGTRAQ	http://www.securityfocus.com/bid/33122
URL	http://www.zerodayinitiative.com/advisories/ZDI-09-001/
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-09-002/
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/94.html
URL	http://www.reversemode.com/index.php? option=com_content&task=view&id=54&Itemid=1

MS10-012 Vulnerabilities In SMB Server Allow Remote Code Execution (Network Check)	Medium

Vulnerability Details

The Microsoft Windows implementation of the Server Message Block (SMB) protocol fails to provide enough entropy to the NTLM authentication mechanism. This flaw in the SMB implementation allows duplicate nonces to be issued by the authenticating server, which can in turn be leveraged by an attacker to gain access to the system without knowledge of system credentials.

A nonce is an authentication challenge that should not be used more than once, and is an essential component of SMB NTLM authentication which allows users to authenticate with remote SMB servers.

An attacker can use a duplicate nonce in a replay attack which will allow him to be authenticated by the vulnerable server. Once authenticated, the attacker can perform actions under the context of the account that was used to gain access to the server.

The presence of this vulnerability implies the absence of Microsoft patch MS10-012 as well as the existence of several other vulnerabilities in the SMB implementation. The other vulnerabilities include an unauthenticated memory corruption flaw, an unauthenticated null pointer denial of service flaw, and an authenticated pathname overflow flaw.
Impact:
The MS10-012 patch provides a fix for multiple vulnerabilities that are present in the SMB implementation. Each of the vulnerabilities has a different level of impact. The impact ranges from initiating a denial of service condition on the vulnerable host, to gaining complete access to the machine and other hosts on the network.

Solution Details

Microsoft has released updates to address this issue. If automatic updating is not enabled, please obtain the appropriate update as described in the MS10-012 Security Bulletin linked in the References List of the vulnerability details. Hosts connected to the Internet should have a minimal number of ports exposed. All unsolicited inbound communication from the Internet should be blocked as well. A workaround is to block TCP ports 139 and 445 which are used by the affected component, although other applications or services using these ports may be interrupted.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0231
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0022
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0020
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0021

Type	Reference
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://cwe.mitre.org/data/definitions/362.html

MS11-020: SMB Transaction Parsing Vulnerability (Network Check) — Medium

Vulnerability Details

This instance of the Microsoft SMB Server service contains an SMB transaction parsing vulnerability. A remote attacker can leverage this flaw to execute arbitrary code on the vulnerable host.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft patch MS11-020 addresses this vulnerability. Apply MS11-020 to the vulnerable system either directly or through the standard Microsoft Update mechanism.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-0661
BUGTRAQ	http://www.securityfocus.com/bid/47198
URL	https://cwe.mitre.org/data/definitions/20.html

MS14-085: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure — Medium

Vulnerability Details

This security update resolves a publicly disclosed vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if a user browses to a website containing specially crafted JPEG content. An attacker could use this information disclosure vulnerability to gain information about the system that could then be combined with other attacks to compromise the system. The information disclosure vulnerability by itself does not allow arbitrary code execution. However, an attacker could use this information disclosure vulnerability in conjunction with another vulnerability to bypass security features such as Address Space Layout Randomization (ASLR).

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS14-

085'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS14-085' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6355
MSB	http://technet.microsoft.com/security/bulletin/MS14-085
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS14-085

MS15-001: Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-001' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-001'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0002
BUGTRAQ	http://www.securityfocus.com/bid/71972
MSB	http://technet.microsoft.com/security/bulletin/MS15-001
URL	http://www.zdnet.com/article/google-discloses-unpatched-windows-vulnerability/
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-001
URL	https://code.google.com/p/google-security-research/issues/detail?id=118

MS15-003: Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege

Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-003'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-003' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0004
BUGTRAQ	http://www.securityfocus.com/bid/71967
MSB	http://technet.microsoft.com/security/bulletin/MS15-003

Type	Reference
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-003
URL	https://code.google.com/p/google-security-research/issues/detail?id=123

MS15-004: Vulnerability in Windows Components Could Allow Elevation of Privilege

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-004' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-004'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0016
BUGTRAQ	http://www.securityfocus.com/bid/71965
MSB	http://technet.microsoft.com/security/bulletin/MS15-004
URL	https://cwe.mitre.org/data/definitions/22.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-004
URL	http://blog.trendmicro.com/trendlabs-security-intelligence/cve-2015-0016-escaping-the-internet-explorer-sandbox/
URL	http://packetstormsecurity.com/files/130201/MS15-004-Microsoft-Remote-Desktop-Services-Web-Proxy-IE-Sandbox-Escape.html

MS15-005: Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-005' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Security Bypass' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-005'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2

- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.1

CVSS Vector: AV:A/AC:L/Au:N/C:N/I:C/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0006
BUGTRAQ	http://www.securityfocus.com/bid/71930
MSB	http://technet.microsoft.com/security/bulletin/MS15-005
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-005

MS15-006: Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-006' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Security Bypass' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-006'.

Affected Products Are:
- Windows 8
- Windows 8.1
- Windows RT

- Windows RT 8.1
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

CVSS Base Score: 1.9

CVSS Vector: AV:L/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0001
BUGTRAQ	http://www.securityfocus.com/bid/71927
MSB	http://technet.microsoft.com/security/bulletin/MS15-006
URL	http://packetstormsecurity.com/files/134392/Microsoft-Windows-8.1-Ahcache.sys-NtApphelpCacheControl-Privilege-Escalation.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-006

MS15-007: Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service — Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-007' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Denial of Service' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-007'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0015
BUGTRAQ	http://www.securityfocus.com/bid/71933
MSB	http://technet.microsoft.com/security/bulletin/MS15-007
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-007
URL	https://cwe.mitre.org/data/definitions/399.html

MS15-014: Vulnerability in Group Policy Could Allow Security Feature Bypass

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-014' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Security Bypass' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-014'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1

- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 3.3

CVSS Vector: AV:A/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0009
BUGTRAQ	http://www.securityfocus.com/bid/72476
MSB	http://technet.microsoft.com/security/bulletin/MS15-014
URL	http://blogs.technet.com/b/srd/archive/2015/02/10/ms15-011-amp-ms15-014-hardening-group-policy.aspx
URL	https://cwe.mitre.org/data/definitions/254.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-014

MS15-015: Vulnerability in Microsoft Windows Could Allow Elevation of Privilege

Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-015' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-015'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0062
BUGTRAQ	http://www.securityfocus.com/bid/72458
MSB	http://technet.microsoft.com/security/bulletin/MS15-015
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-015

MS15-016: Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-016' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-016'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0061
BUGTRAQ	http://www.securityfocus.com/bid/72456
MSB	http://technet.microsoft.com/security/bulletin/MS15-016
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-016

MS15-023: Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-023' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-023'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0094
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0077
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0078
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0095
BUGTRAQ	http://www.securityfocus.com/bid/72897
BUGTRAQ	http://www.securityfocus.com/bid/72936
MSB	http://technet.microsoft.com/security/bulletin/MS15-023
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-023

Type	Reference
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/476.html

MS15-025: Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-025' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-025'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0073
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0075
BUGTRAQ	http://www.securityfocus.com/bid/72915
BUGTRAQ	http://www.securityfocus.com/bid/72908
MSB	http://technet.microsoft.com/security/bulletin/MS15-025
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-025

MS15-027: Vulnerability in NETLOGON Could Allow Spoofing — Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-027' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Spoofing' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-027'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:A/AC:M/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0005
MSB	http://technet.microsoft.com/security/bulletin/MS15-027
URL	https://cwe.mitre.org/data/definitions/254.html
URL	http://packetstormsecurity.com/files/130773/Windows-Pass-Through-Authentication-Methods-Improper-Validation.html
URL	http://www.coresecurity.com/advisories/windows-pass-through-authentication-methods-improper-validation
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-027
URL	https://www.samba.org/samba/history/samba-4.2.10.html

MS15-028: Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass

Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-028' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Security Bypass' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-028'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

CVSS Base Score: 2.1

CVSS Vector: AV:L/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0084
BUGTRAQ	http://www.securityfocus.com/bid/72913
MSB	http://technet.microsoft.com/security/bulletin/MS15-028
URL	https://cwe.mitre.org/data/definitions/254.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-028

MS15-029: Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-029' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-029'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0076
BUGTRAQ	http://www.securityfocus.com/bid/72918
MSB	http://technet.microsoft.com/security/bulletin/MS15-029
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-029
URL	https://cwe.mitre.org/data/definitions/200.html

MS15-030: Vulnerability in Remote Desktop Protocol Could Allow Denial of Service

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-030' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Denial of Service' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-030'.

Affected Products Are:
- Windows 7

- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

CVSS Base Score: 7.8

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0079
MSB	http://technet.microsoft.com/security/bulletin/MS15-030
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-030
URL	https://cwe.mitre.org/data/definitions/399.html

MS15-031: Vulnerability in Schannel Could Allow Security Feature Bypass

Medium

Vulnerability Details

The remote Windows host is affected by a 'Security Bypass' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to knock it offline, denying service to legitimate users.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-031'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2

- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-031' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1637
BUGTRAQ	http://www.securityfocus.com/bid/72965
MSB	http://technet.microsoft.com/security/bulletin/MS15-031
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-031
URL	https://cwe.mitre.org/data/definitions/310.html
URL	https://technet.microsoft.com/library/security/3046015

MS15-038: Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege — Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-038' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-038'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2003 R2
- Windows Server 2003 R2 x64 Edition
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1644
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1643
BUGTRAQ	http://www.securityfocus.com/bid/73998
MSB	http://technet.microsoft.com/security/bulletin/MS15-038
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-038

MS15-041: Vulnerability in .NET Framework Could Allow Information Disclosure

Medium

Vulnerability Details

The remote Windows host is affected by a 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-041'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-041' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine. This patch does not require a reboot.

CVSS Base Score: 2.6

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1648
MSB	http://technet.microsoft.com/security/bulletin/MS15-041
URL	https://cwe.mitre.org/data/definitions/19.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-041

MS15-048: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege

Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-048' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-048'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1673
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1672
BUGTRAQ	http://www.securityfocus.com/bid/74487
BUGTRAQ	http://www.securityfocus.com/bid/74482
MSB	http://technet.microsoft.com/security/bulletin/MS15-048

Type	Reference
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-048
URL	https://cwe.mitre.org/data/definitions/310.html

MS15-050: Vulnerability in Service Control Manager Could Allow Elevation of Privilege

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-050'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-050' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 6.9

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1702
BUGTRAQ	http://www.securityfocus.com/bid/74492
MSB	http://technet.microsoft.com/security/bulletin/MS15-050
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-050

MS15-051: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-051' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-051'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1676
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1680
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1701
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1677
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1679
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1678
BUGTRAQ	http://www.securityfocus.com/bid/74494
BUGTRAQ	http://www.securityfocus.com/bid/74483
BUGTRAQ	http://www.securityfocus.com/bid/74496
BUGTRAQ	http://www.securityfocus.com/bid/74497
BUGTRAQ	http://www.securityfocus.com/bid/74245
BUGTRAQ	http://www.securityfocus.com/bid/74495
MSB	http://technet.microsoft.com/security/bulletin/MS15-051
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-051
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://www.fireeye.com/blog/threat-research/2015/04/probable_apt28_useo.html

MS15-052: Vulnerability in Windows Kernel Could Allow Security Feature Bypass — Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-052' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Security Bypass' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-052'.

Affected Products Are:
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.6

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1674
BUGTRAQ	http://www.securityfocus.com/bid/74488
MSB	http://technet.microsoft.com/security/bulletin/MS15-052
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-052
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/20.html

MS15-055: Vulnerability in Schannel Could Allow Information Disclosure

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-055' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to knock it offline, denying service to legitimate users.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-055'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1716
BUGTRAQ	http://www.securityfocus.com/bid/74489
MSB	http://technet.microsoft.com/security/bulletin/MS15-055
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/310.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-055

MS15-060: Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-060' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-060'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1756
BUGTRAQ	http://www.securityfocus.com/bid/75017
MSB	http://technet.microsoft.com/security/bulletin/MS15-060
URL	https://cwe.mitre.org/data/definitions/416.html

Type	Reference
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-060

MS15-061: Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege	Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-061' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-061'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2003 R2
- Windows Server 2003 R2 x64 Edition
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1723
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1722
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1721
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1720
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1719
MSB	http://technet.microsoft.com/security/bulletin/MS15-061
URL	https://cwe.mitre.org/data/definitions/416.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/476.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-061

MS15-071: Vulnerability in Netlogon Could Allow Elevation of Privilege

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-071'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2003 R2
- Windows Server 2003 R2 x64 Edition
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-071' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 3.3

CVSS Vector: AV:A/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2374
BUGTRAQ	http://www.securityfocus.com/bid/75633
MSB	http://technet.microsoft.com/security/bulletin/MS15-071
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-071

MS15-072: Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-072'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8

- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2003 R2
- Windows Server 2003 R2 x64 Edition
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-072' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2364
MSB	http://technet.microsoft.com/security/bulletin/MS15-072
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-072

MS15-073: Vulnerabilities in Windows Kernel-Mode Driver Could Allow Elevation of Privilege

Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-073' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-073'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2003 R2
- Windows Server 2003 R2 x64 Edition
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2367
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2365
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2381
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2366
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2363
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2382
MSB	http://technet.microsoft.com/security/bulletin/MS15-073
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-073
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-536

Type	Reference
URL	https://cwe.mitre.org/data/definitions/200.html

MS15-075: Vulnerabilities in OLE Could Allow Elevation of Privilege — Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-075'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-075' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2417

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2416
MSB	http://technet.microsoft.com/security/bulletin/MS15-075
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-075

MS15-076: Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-076'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2003 R2
- Windows Server 2003 R2 x64 Edition
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-076' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2370
MSB	http://technet.microsoft.com/security/bulletin/MS15-076
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-076

MS15-077: Vulnerability in ATM Font Driver Could Allow Elevation of Privilege

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-077' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-077'.

Affected Products Are:
- Microsoft Windows Server 2003
- Microsoft Windows Server 2003 x64 Edition
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2

- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2387
BUGTRAQ	http://www.securityfocus.com/bid/75587
MSB	http://technet.microsoft.com/security/bulletin/MS15-077
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-077

MS15-082: Vulnerabilities in RDP Could Allow Remote Code Execution Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-082' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-082'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)

- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2472
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2473
MSB	http://technet.microsoft.com/security/bulletin/MS15-082
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-082
URL	https://cwe.mitre.org/data/definitions/20.html

MS15-084: Vulnerabilities in XML Core Services Could Allow Information Disclosure

Medium

Vulnerability Details

The remote Windows host is affected by a 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-084'.

Affected Products Are:
- Microsoft InfoPath 2007
- Microsoft Office 2007
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-084' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2471
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2434
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2440
BUGTRAQ	http://www.securityfocus.com/bid/76232
MSB	http://technet.microsoft.com/security/bulletin/MS15-084
URL	http://www.zerodayinitiative.com/advisories/ZDI-15-381
URL	https://cwe.mitre.org/data/definitions/310.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-084
URL	https://cwe.mitre.org/data/definitions/200.html

MS15-085: Vulnerability in Mount Manager Could Allow Elevation of Privilege

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-085'.

Affected Products Are:
- Windows 10
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-085' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1769
MSB	http://technet.microsoft.com/security/bulletin/MS15-085
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-085
URL	http://blogs.technet.com/b/srd/archive/2015/08/11/defending-against-cve-2015-1769-a-logical-issue-exploited-via-a-malicious-usb-stick.aspx
URL	https://cwe.mitre.org/data/definitions/59.html

MS15-088: Unsafe Command Line Parameter Passing Could Allow Information Disclosure

Medium

Vulnerability Details

The remote Windows host is affected by a 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-088'.

Affected Products Are:
- Windows 10
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-088' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2423
MSB	http://technet.microsoft.com/security/bulletin/MS15-081
MSB	http://technet.microsoft.com/security/bulletin/MS15-088
MSB	http://technet.microsoft.com/security/bulletin/MS15-079
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-088
URL	https://cwe.mitre.org/data/definitions/200.html

MS15-092: Vulnerabilities in .NET Framework Could Allow Elevation of Privilege

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-092'.

Affected Products Are:
- Windows 10
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-092' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2480
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2479

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2481
MSB	http://technet.microsoft.com/security/bulletin/MS15-092
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-092

MS15-102: Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-102'.

Affected Products Are:
- Windows 10
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-102' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2525
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2524
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2528
BUGTRAQ	http://www.securityfocus.com/bid/76653
MSB	http://technet.microsoft.com/security/bulletin/MS15-102
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-102

MS15-119: Security Update for Winsock to Address Elevation of Privilege

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-119'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-119' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2478
MSB	http://technet.microsoft.com/security/bulletin/MS15-119

MS15-120: Security Update for IPSec to Address Denial of Service Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-120' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Denial of Service' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-120'.

Affected Products Are:
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:L/Au:S/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6111
MSB	http://technet.microsoft.com/security/bulletin/MS15-120
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-120

MS15-121: Security Update for Schannel to Address Spoofing

Medium

Vulnerability Details

The remote Windows host is affected by a 'Spoofing' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to knock it offline, denying service to legitimate users.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-121'.

Affected Products Are:
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-121' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6112
MSB	http://technet.microsoft.com/security/bulletin/MS15-121
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-121

MS15-122: Security Update for Kerberos to Address Security Feature Bypass — Medium

Vulnerability Details

The remote Windows host is affected by a 'Security Bypass' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-122'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-122' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 4.9

CVSS Vector: AV:L/AC:L/Au:N/C:N/I:C/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6095
MSB	http://technet.microsoft.com/security/bulletin/MS15-122
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-122
URL	https://cwe.mitre.org/data/definitions/255.html

MS15-132: Security Update for Microsoft Windows to Address Remote Code Execution

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-132' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-132'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6133
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6128
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6132
BUGTRAQ	http://www.securityfocus.com/bid/78612
MSB	http://technet.microsoft.com/security/bulletin/MS15-132
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-132

MS15-133: Security Update for Windows PGM to Address Elevation of Privilege — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS15-133'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS15-133' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.2

CVSS Vector: AV:L/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6126
MSB	http://technet.microsoft.com/security/bulletin/MS15-133
URL	https://cwe.mitre.org/data/definitions/362.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS15-133

MS16-007: Security Update for Microsoft Windows to Address Remote Code Execution

Medium

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-007'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-007' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 8.1

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0014
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0015
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0016
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0018
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0019
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0020
MSB	http://technet.microsoft.com/security/bulletin/MS16-007
URL	https://cwe.mitre.org/data/definitions/426.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	http://packetstormsecurity.com/files/135232/Microsoft-DirectShow-Remote-Code-Execution.html
URL	https://code.google.com/p/google-security-research/issues/detail?id=555
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-018
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-007
URL	https://cwe.mitre.org/data/definitions/119.html

MS16-008: Security Update for Windows Kernel to Address Elevation of Privilege

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-008' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-008'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8
- Windows 8.1
- Windows RT
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.3

CVSS Vector: AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0006
BUGTRAQ	http://www.securityfocus.com/bid/79882

Type	Reference
MSB	http://technet.microsoft.com/security/bulletin/MS16-008
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-008

MS16-014: Security Update for Microsoft Windows to Address Remote Code Execution

Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-014' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-014'.

Affected Products Are:
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0041

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0040
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0044
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0042
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0049
BUGTRAQ	http://www.securityfocus.com/bid/82535
MSB	http://technet.microsoft.com/security/bulletin/MS16-009
MSB	http://technet.microsoft.com/security/bulletin/MS16-014
URL	https://cwe.mitre.org/data/definitions/255.html
URL	https://www.securify.nl/advisory/SFY20150905/nps_datastore_server_dll_side_loading_vulnerability.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-014
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://packetstormsecurity.com/files/135797/Windows-Kerberos-Security-Feature-Bypass.html

MS16-018: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege

Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-018' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-

018'.

Affected Products Are:
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0048
MSB	http://technet.microsoft.com/security/bulletin/MS16-018
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-018

MS16-021: Security Update for NPS RADIUS Server to Address Denial of Service — Medium

Vulnerability Details

The remote Windows host is affected by a 'Denial of Service' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to knock it offline, denying service to legitimate users.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-021'.

Affected Products Are:
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-021' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.3

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0050
MSB	http://technet.microsoft.com/security/bulletin/MS16-021
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-021

MS16-032: Security Update for Secondary Logon to Address Elevation of Privile

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-032'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-032' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0099
BUGTRAQ	http://www.securityfocus.com/bid/84034
MSB	http://technet.microsoft.com/security/bulletin/MS16-032
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-032

MS16-033: Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege

Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-033' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise it's security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-033'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)

- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0133
BUGTRAQ	http://www.securityfocus.com/bid/84035
MSB	http://technet.microsoft.com/security/bulletin/MS16-033
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-033

MS16-034: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege

Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-034'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-034' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0093
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0096
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0095
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0094
BUGTRAQ	http://www.securityfocus.com/bid/84072
BUGTRAQ	http://www.securityfocus.com/bid/84054
BUGTRAQ	http://www.securityfocus.com/bid/84069
BUGTRAQ	http://www.securityfocus.com/bid/84066
MSB	http://technet.microsoft.com/security/bulletin/MS16-034
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-034
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-196

MS16-047: Windows SAM and LSAD Downgrade Vulnerability - Badlock (Network Check) Medium

Solution Details

Apply the update provided by the vendor to address this issue. If you are using an operating system that is no longer supported, upgrade the asset to a supported operating system in order to obtain a patch for this vulnerability.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This asset is vulnerable to a privilege escalation Man in The Middle (MiTM) attack due to SAM and LSAD RPC services permitting weak authentication levels, which do not provide adequate protection, during channel establishment.
Impact:
A remote, unauthenticated attacker in position to perform a Man in The Middle (MiTM) attack could intercept a legitimate user's traffic, force a downgrade of the authentication level then impersonate that user, with access to all privileges available to that user.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0128
MSB	http://technet.microsoft.com/security/bulletin/MS16-047
URL	https://www.samba.org/samba/security/CVE-2016-2118.html
URL	https://bto.bluecoat.com/security-advisory/sa122
URL	https://cwe.mitre.org/data/definitions/254.html

MS16-048: Security Update for CSRSS — Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-048' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Security Bypass' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-048'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 8.1

- Windows RT 8.1
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0151
MSB	http://technet.microsoft.com/security/bulletin/MS16-048
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-048

MS16-060: Security Update for Windows Kernel — Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-060'.

Affected Products Are:
- Microsoft Windows Server 2003
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2

- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-060' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0180
BUGTRAQ	http://www.securityfocus.com/bid/90028
MSB	http://technet.microsoft.com/security/bulletin/MS16-060
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-060

MS16-061: Security Update for Microsoft RPC — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-061'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows Server 2008

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-061' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0178
BUGTRAQ	http://www.securityfocus.com/bid/90032
MSB	http://technet.microsoft.com/security/bulletin/MS16-061
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-061

MS16-065: Security Update for .NET Framework — Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-065' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by an 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-065'.

Affected Products Are:
- Windows 7

- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0149
BUGTRAQ	http://www.securityfocus.com/bid/90026
MSB	http://technet.microsoft.com/security/bulletin/MS16-065
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-065

MS16-072: Security Update for Group Policy — Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-072'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)

- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-072' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.1

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3223
MSB	http://technet.microsoft.com/security/bulletin/MS16-072
URL	http://packetstormsecurity.com/files/138248/Microsoft-Windows-7-Group-Policy-Privilege-Escalation.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-072

MS16-073: Security Update for Windows Kernel-Mode Drivers — Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-073' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-073'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3221
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3232
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3218
MSB	http://technet.microsoft.com/security/bulletin/MS16-073
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-073
URL	https://cwe.mitre.org/data/definitions/200.html

MS16-074: Security Update for Microsoft Graphics Component — Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-074'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7

- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-074' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3219
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3220
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3216
MSB	http://technet.microsoft.com/security/bulletin/MS16-074
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-074
URL	https://cwe.mitre.org/data/definitions/200.html

MS16-075: Security Update for Windows SMB Server — Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-075'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-075' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3225
MSB	http://technet.microsoft.com/security/bulletin/MS16-075
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-075

MS16-076: Security Update for Netlogon — Medium

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-076'.

Affected Products Are:
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-076' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3228
MSB	http://technet.microsoft.com/security/bulletin/MS16-076
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-076
URL	https://cwe.mitre.org/data/definitions/20.html

MS16-077: Security Update for WPAD — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-077'.

Affected Products Are:
- Windows 10

- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-077' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3213
MSB	http://technet.microsoft.com/security/bulletin/MS16-063
MSB	http://technet.microsoft.com/security/bulletin/MS16-077
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-077

MS16-080: Security Update for Microsoft Windows PDF — Medium

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-080'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-080' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3215
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3201
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3203
BUGTRAQ	http://www.securityfocus.com/bid/91086
MSB	http://technet.microsoft.com/security/bulletin/MS16-068
MSB	http://technet.microsoft.com/security/bulletin/MS16-080
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-370
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-369
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-080

MS16-082: Security Update for Microsoft Windows Search Component Medium

Vulnerability Details

The remote Windows host is affected by a 'Denial of Service' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker to send malformed input to the affected service to knock it offline, denying service to legitimate users.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-082'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-082' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 5

CVSS Vector: AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3230
MSB	http://technet.microsoft.com/security/bulletin/MS16-082
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-082

MS16-090: Security Update for Windows Kernel-Mode Drivers — Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-090'.

Affected Products Are:
- Windows 10

- Windows 10 Version 1511
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-090' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3250
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3252
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3251
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3254
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3286
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3249
BUGTRAQ	http://www.securityfocus.com/bid/91597
BUGTRAQ	http://www.securityfocus.com/bid/91615
BUGTRAQ	http://www.securityfocus.com/bid/91613
BUGTRAQ	http://www.securityfocus.com/bid/91614
BUGTRAQ	http://www.securityfocus.com/bid/91616
MSB	http://technet.microsoft.com/security/bulletin/MS16-090

Type	Reference
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-090

MS16-092: Security Update for Windows Kernel — Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-092' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Security Bypass' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-092'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.7

CVSS Vector: AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3272
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3258
BUGTRAQ	http://www.securityfocus.com/bid/91603

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/91606
MSB	http://technet.microsoft.com/security/bulletin/MS16-092
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-092

MS16-111: Security Update for Windows Kernel

Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-111'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-111' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3371
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3373
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3306
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3305
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3372
BUGTRAQ	http://www.securityfocus.com/bid/92815
BUGTRAQ	http://www.securityfocus.com/bid/92813
BUGTRAQ	http://www.securityfocus.com/bid/92812
BUGTRAQ	http://www.securityfocus.com/bid/92845
BUGTRAQ	http://www.securityfocus.com/bid/92814
MSB	http://technet.microsoft.com/security/bulletin/MS16-111
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-111
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/200.html

MS16-112: Security Update for Windows Lock Screen — Medium

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-112' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-112'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.3

CVSS Vector: AV:P/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3302
BUGTRAQ	http://www.securityfocus.com/bid/92853
MSB	http://technet.microsoft.com/security/bulletin/MS16-112
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-112

MS16-114: Security Update for Windows SMBv1 Server — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote Windows host is affected by a 'Remote Code Execution' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-114'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7

- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their 'MS16-114' update. Please download and install the patch from Microsoft Technet or run Windows Update on the affected machine.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3345
BUGTRAQ	http://www.securityfocus.com/bid/92859
MSB	http://technet.microsoft.com/security/bulletin/MS16-114
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-114
URL	https://cwe.mitre.org/data/definitions/284.html

MS16-134: Security Update for Common Log File System Driver — Medium

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-134'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7

- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their November 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7184
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3343
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3342
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3340
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3338
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3335
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3334
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3333
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3332
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0026
BUGTRAQ	http://www.securityfocus.com/bid/94009
BUGTRAQ	http://www.securityfocus.com/bid/94015

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/94007
BUGTRAQ	http://www.securityfocus.com/bid/94013
BUGTRAQ	http://www.securityfocus.com/bid/94010
BUGTRAQ	http://www.securityfocus.com/bid/94014
BUGTRAQ	http://www.securityfocus.com/bid/94011
BUGTRAQ	http://www.securityfocus.com/bid/94012
BUGTRAQ	http://www.securityfocus.com/bid/94008
BUGTRAQ	http://www.securityfocus.com/bid/93998
MSB	http://technet.microsoft.com/security/bulletin/MS16-134
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-134

MS16-135: Security Update for Windows Kernel-Mode Drivers — Medium

Solution Details

Microsoft has released a fix for this flaw in their November 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-135'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7218
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7246
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7255
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7214
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7215
BUGTRAQ	http://www.securityfocus.com/bid/94004
BUGTRAQ	http://www.securityfocus.com/bid/94063
BUGTRAQ	http://www.securityfocus.com/bid/94000
BUGTRAQ	http://www.securityfocus.com/bid/93991
BUGTRAQ	http://www.securityfocus.com/bid/94064
MSB	http://technet.microsoft.com/security/bulletin/MS16-135
URL	https://github.com/mwrlabs/CVE-2016-7255
URL	http://packetstormsecurity.com/files/140468/Microsoft-Windows-Kernel-win32k.sys-NtSetWindowLongPtr-Privilege-Escalation.html
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-594
URL	https://securingtomorrow.mcafee.com/mcafee-labs/digging-windows-kernel-privilege-escalation-vulnerability-cve-2016-7255/

Type	Reference
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://blog.trendmicro.com/trendlabs-security-intelligence/one-bit-rule-system-analyzing-cve-2016-7255-exploit-wild/
URL	https://security.googleblog.com/2016/10/disclosing-vulnerabilities-to-protect.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-135
URL	http://www.zerodayinitiative.com/advisories/ZDI-16-592

MS16-138: Security Update to Microsoft Virtual Hard Drive — Medium

Solution Details

Microsoft has released a fix for this flaw in their November 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-138'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 8.1
- Windows RT 8.1
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.1

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7224
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7225
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7226
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7223
BUGTRAQ	http://www.securityfocus.com/bid/94018
BUGTRAQ	http://www.securityfocus.com/bid/94003
BUGTRAQ	http://www.securityfocus.com/bid/94017
BUGTRAQ	http://www.securityfocus.com/bid/94016
MSB	http://technet.microsoft.com/security/bulletin/MS16-138
URL	https://cwe.mitre.org/data/definitions/284.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-138

MS16-149: Security Update for Windows — Medium

Solution Details

Microsoft has released a fix for this flaw in their December 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow a remote attacker to leverage malformed input to the affected component to execute arbitrary code with the privileges of the running process.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-149'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1

- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7292
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7219
BUGTRAQ	http://www.securityfocus.com/bid/94764
BUGTRAQ	http://www.securityfocus.com/bid/94768
MSB	http://technet.microsoft.com/security/bulletin/MS16-149
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-149
URL	https://cwe.mitre.org/data/definitions/19.html

MS16-151: Security Update for Kernel-Mode Driver — Medium

Solution Details

Microsoft has released a fix for this flaw in their December 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-151'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7259
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7260
BUGTRAQ	http://www.securityfocus.com/bid/94785
BUGTRAQ	http://www.securityfocus.com/bid/94771
MSB	http://technet.microsoft.com/security/bulletin/MS16-151
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-151
URL	https://cwe.mitre.org/data/definitions/19.html
URL	http://blog.quarkslab.com/cve-2016-7259-an-empty-file-into-the-blue.html
URL	http://packetstormsecurity.com/files/140172/Microsoft-Windows-Type-1-Font-Processing-Privilege-Escalation.html

MS16-153: Security Update for Common Log File System Driver — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their December 2016 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS16-153'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (server core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 5.5

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7295
BUGTRAQ	http://www.securityfocus.com/bid/94787
MSB	http://technet.microsoft.com/security/bulletin/MS16-153

Type	Reference
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS16-153

MS17-016: Security Update for Windows IIS — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their March 2017 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS17-016'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 6.1

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0055
BUGTRAQ	http://www.securityfocus.com/bid/96622
URL	https://cwe.mitre.org/data/definitions/79.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0055

MS17-017: Security Update for Windows Kernel — Medium

Solution Details

Microsoft has released a fix for this flaw in their March 2017 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS17-017'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0050
BUGTRAQ	http://www.securityfocus.com/bid/96025
URL	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-017
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0050

MS17-018: Security Update for Windows Kernel-Mode Drivers — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their March 2017 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

The remote Windows host is affected by a 'Elevation of Privilege' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker with unprivileged access to the affected component to leverage input validation flaws to upgrade their privileges to that of a privileged user

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS17-018'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2

- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0024
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0082
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0026
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0056
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0078
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0079
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0080
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0081
BUGTRAQ	http://www.securityfocus.com/bid/96631
BUGTRAQ	http://www.securityfocus.com/bid/96634
BUGTRAQ	http://www.securityfocus.com/bid/96029
BUGTRAQ	http://www.securityfocus.com/bid/96032
BUGTRAQ	http://www.securityfocus.com/bid/96630
BUGTRAQ	http://www.securityfocus.com/bid/96632
BUGTRAQ	http://www.securityfocus.com/bid/96633
BUGTRAQ	http://www.securityfocus.com/bid/96635
URL	http://technet.microsoft.com/en-us/security/bulletin/MS17-018
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0026
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0056

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0078
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0082
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0079
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0080
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0081
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0024

MS17-021: Security Update for Windows DirectShow

Medium

Vulnerability Details

The remote Windows host is affected by a 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS17-021'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their March 2017 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 3.1

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0042
BUGTRAQ	http://www.securityfocus.com/bid/96098
URL	http://pastebin.com/raw/Eztknq4s
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0042
URL	http://technet.microsoft.com/en-us/security/bulletin/MS17-021
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://twitter.com/Qab/status/842506404950917120

MS17-022: Security Update for Microsoft XML Core Services — Medium

Vulnerability Details

The remote Windows host is affected by a 'Information Disclosure' flaw which could compromise its security posture.

The vulnerability in question could allow an attacker sending malformed input to the affected service to force it to disclose sensitive information not normally available.

Microsoft has rated this flaw 'Important' and released a fix for this in Microsoft Security Bulletin 'MS17-022'.

Affected Products Are:
- Windows 10
- Windows 10 Version 1511
- Windows 10 Version 1607
- Windows 7
- Windows 8.1
- Windows RT 8.1
- Windows Server 2008
- Windows Server 2008 R2

- Windows Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Vista
- Windows Vista x64 Edition

Solution Details

Microsoft has released a fix for this flaw in their March 2017 Quality Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0022
URL	https://0patch.blogspot.com/2017/09/exploit-kit-rendezvous-and-cve-2017-0022.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://technet.microsoft.com/en-us/security/bulletin/MS17-022
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0022

MS17-AUG: Microsoft Internet Explorer Security Update — Medium

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-8625 - Internet Explorer Security Feature Bypass Vulnerability
CVE-2017-8651 - Internet Explorer Memory Corruption Vulnerability

Affected Products:
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 for 32-bit Systems

Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

Solution Details

Microsoft has released a fix for this flaw in their August 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8625
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8651
BUGTRAQ	http://www.securityfocus.com/bid/100058
BUGTRAQ	http://www.securityfocus.com/bid/100063
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://posts.specterops.io/umci-vs-internet-explorer-exploring-cve-2017-8625-3946536c6442
URL	https://msitpros.com/?p=3909
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8651
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4034660
URL	https://support.microsoft.com/en-us/help/4034665
URL	https://support.microsoft.com/en-us/help/4034733
URL	https://support.microsoft.com/en-us/help/4034668
URL	https://support.microsoft.com/en-us/help/4034658

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8625

MS17-JUN: Microsoft Internet Explorer Security Update — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their June 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2017-8519 - Internet Explorer Memory Corruption Vulnerability
CVE-2017-8547 - Internet Explorer Memory Corruption Vulnerability

Affected Products:
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1511 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1511 for 32-bit Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8519
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8547
BUGTRAQ	http://www.securityfocus.com/bid/98899
BUGTRAQ	http://www.securityfocus.com/bid/98932
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8519
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4021558
URL	https://support.microsoft.com/en-us/help/4022719
URL	https://support.microsoft.com/en-us/help/4022724
URL	https://support.microsoft.com/en-us/help/4022725
URL	https://support.microsoft.com/en-us/help/4022726
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8547
URL	https://support.microsoft.com/en-us/help/4022714

MS17-JUN: Microsoft Internet Explorer Security Update - Registry Entry Not Set

Medium

Solution Details

To remedy this vulnerability, the system administrator will need to add a single specific registry entry for 32 bit systems and two registry entries for 64 bit systems.

For 32-bit and 64-bit systems:
Click Start, click Run, type regedt32 or type regedit, and then click OK.
In Registry Editor, locate the following registry folder:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl
Right-click FeatureControl, point to New, and then click Key.
Type FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX, and then press Enter to name the new subkey.
Right-click FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX, point to New, and then click DWORD Value.
Type “iexplore.exe” (without quotes) for the new DWORD value.
Double-click the new DWORD value named iexplore.exe and change the Value data field to 1.
Click OK to close.

For 64-bit systems only:
Click Start, click Run, type regedt32 or type regedit, and then click OK.
In Registry Editor, locate the following registry folder:
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl
Right-click FeatureControl, point to New, and then click Key.
Type FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX, and then press Enter to name the new subkey.
Right-click FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX, point to New, and then click DWORD Value.
Type “iexplore.exe” (without quotes) for the new DWORD value.
Double-click the new DWORD value named iexplore.exe and change the Value data field to 1.
Click OK to close.

Vulnerability Details

The patch for MS17-JUN: Microsoft Internet Explorer Security Update is installed, however, the registry entry in order to be fully protected is not set.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.5

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8529
BUGTRAQ	http://www.securityfocus.com/bid/98953
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8529

MS17-MAY: Microsoft .NET Security Update — Medium

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft has released a security update for Microsoft .NET Framework which includes fixes for the following vulnerabilities:

CVE-2017-0248 - .Net Security Feature Bypass Vulnerability

Affected Products:
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.5.2 on Windows RT 8.1
Microsoft .NET Framework 4.6.2 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 4.6.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.6.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for 32-bit Systems
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.6.2 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 4.6.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6.2 on Windows Server 2012 R2
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6.2 on Windows Server 2012
Microsoft .NET Framework 4.6.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.5.2 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for 32-bit Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.6.2 on Windows RT 8.1
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows Server 2016
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2012
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows Server 2012 R2
Microsoft .NET Framework 4.6/4.6.1 on Windows 8.1 for x64-based systems

Microsoft .NET Framework 4.6.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.6.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2
Microsoft .NET Framework 4.6.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 4.6.2 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 4.6 on Windows 10 for x64-based Systems
Microsoft .NET Framework 4.6.2 on Windows Server 2016
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6/4.6.1 on Windows Server 2012 R2
Microsoft .NET Framework 4.6/4.6.1 on Windows RT 8.1
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1 on Windows 8.1 for 32-bit systems

Solution Details

Microsoft has released a fix for this flaw in their May 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-0248
BUGTRAQ	http://www.securityfocus.com/bid/98117
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0248
URL	https://support.microsoft.com/en-us/help/4019115
URL	https://support.microsoft.com/en-us/help/4019112
URL	https://support.microsoft.com/en-us/help/4019113

Type	Reference
URL	https://support.microsoft.com/en-us/help/4019114
URL	https://support.microsoft.com/en-us/help/4019474
URL	https://support.microsoft.com/en-us/help/4016871
URL	https://support.microsoft.com/en-us/help/4019472
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://support.microsoft.com/en-us/help/4019473

MS17-NOV: Microsoft Windows Security Update — Medium

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the following vulnerabilities:

CVE-2017-11788 - Windows Search Denial of Service Vulnerability
CVE-2017-11830 - Device Guard Security Feature Bypass Vulnerability
CVE-2017-11831 - Windows Information Disclosure Vulnerability
CVE-2017-11832 - Windows EOT Font Engine Information Disclosure Vulnerability
CVE-2017-11851 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-11876 - Microsoft Project Server Elevation of Privilege Vulnerability
CVE-2017-11768 - Windows Media Player Information Disclosure Vulnerability
CVE-2017-11835 - Windows EOT Font Engine Information Disclosure Vulnerability
CVE-2017-11842 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-11847 - Windows Kernel Elevation of Privilege Vulnerability
CVE-2017-11849 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-11850 - Microsoft Graphics Component Information Disclosure Vulnerability
CVE-2017-11852 - Windows GDI Information Disclosure Vulnerability
CVE-2017-11853 - Windows Kernel Information Disclosure Vulnerability
CVE-2017-11880 - Windows Information Disclosure Vulnerability

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Microsoft SharePoint Enterprise Server 2016
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows 10 Version 1709 for 64-based Systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1

Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows 8.1 for 32-bit systems
Microsoft Project Server 2013 Service Pack 1
Windows 10 Version 1511 for x64-based Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1511 for 32-bit Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows RT 8.1
Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows Server 2016
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their November 2017 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11852
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11880
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11876
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11842
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11788
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11830
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11832

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11853
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11847
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11849
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11835
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11850
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11831
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11768
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11851
BUGTRAQ	http://www.securityfocus.com/bid/101739
BUGTRAQ	http://www.securityfocus.com/bid/101755
BUGTRAQ	http://www.securityfocus.com/bid/101719
BUGTRAQ	http://www.securityfocus.com/bid/101711
BUGTRAQ	http://www.securityfocus.com/bid/101714
BUGTRAQ	http://www.securityfocus.com/bid/101726
BUGTRAQ	http://www.securityfocus.com/bid/101764
BUGTRAQ	http://www.securityfocus.com/bid/101729
BUGTRAQ	http://www.securityfocus.com/bid/101762
BUGTRAQ	http://www.securityfocus.com/bid/101754
BUGTRAQ	http://www.securityfocus.com/bid/101736
BUGTRAQ	http://www.securityfocus.com/bid/101738
BUGTRAQ	http://www.securityfocus.com/bid/101705
BUGTRAQ	http://www.securityfocus.com/bid/101721
BUGTRAQ	http://www.securityfocus.com/bid/101763
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11831

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11852
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11880
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11842
URL	https://support.microsoft.com/en-us/help/4048970
URL	https://support.microsoft.com/en-us/help/4047211
URL	https://support.microsoft.com/en-us/help/4011257
URL	https://support.microsoft.com/en-us/help/4048961
URL	https://support.microsoft.com/en-us/help/4011244
URL	https://support.microsoft.com/en-us/help/4048968
URL	https://support.microsoft.com/en-us/help/4048960
URL	https://support.microsoft.com/en-us/help/4046184
URL	https://support.microsoft.com/en-us/help/4048962
URL	https://support.microsoft.com/en-us/help/4049164
URL	https://support.microsoft.com/en-us/help/4048956
URL	https://support.microsoft.com/en-us/help/4048953
URL	https://support.microsoft.com/en-us/help/4048958
URL	https://support.microsoft.com/en-us/help/4048952
URL	https://support.microsoft.com/en-us/help/4048959
URL	https://support.microsoft.com/en-us/help/4048954
URL	https://support.microsoft.com/en-us/help/4048955
URL	https://support.microsoft.com/en-us/help/4048957
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11788

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11830
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11832
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11853
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11847
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11849
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11876
URL	https://cwe.mitre.org/data/definitions/352.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11835
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11850
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11768
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-11851

MS17-SEP: Microsoft Internet Explorer Security Update - Registry Entry Not Set

Medium

Solution Details

To remedy this vulnerability, the system administrator will need to add a single specific registry entry for 32 bit systems and two registry entries for 64 bit systems.

For 32-bit and 64-bit systems:

Click Start, click Run, type regedt32 or type regedit, and then click OK.
In Registry Editor, locate the following registry folder:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Main\FeatureControl
Right-click FeatureControl, point to New, and then click Key.
Type FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX, and then press Enter to name the new subkey.
Right-click FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX, point to New, and then click DWORD Value.
Type “iexplore.exe” for the new DWORD value.
Double-click the new DWORD value named iexplore.exe and change the Value data field to 1.
Click OK to close.

For 64-bit systems only:
Click Start, click Run, type regedt32 or type regedit, and then click OK.
In Registry Editor, locate the following registry folder:
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Internet Explorer\Main\FeatureControl
Right-click FeatureControl, point to New, and then click Key.
Type FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX, and then press Enter to name the new subkey.
Right-click FEATURE_ENABLE_PRINT_INFO_DISCLOSURE_FIX, point to New, and then click DWORD Value.
Type “iexplore.exe” for the new DWORD value.
Double-click the new DWORD value named iexplore.exe and change the Value data field to 1.
Click OK to close.

Vulnerability Details

The patch for MS17-SEP: Microsoft Internet Explorer Security Update is installed, however, the registry entry in order to be fully protected is not set.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-8529
BUGTRAQ	http://www.securityfocus.com/bid/98953
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-8529
URL	https://cwe.mitre.org/data/definitions/200.html

MS18-JAN: Microsoft .NET Security Update

Medium

Solution Details

Microsoft has released a fix for this flaw in their January 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

PLEASE NOTE: If this patch is not being offered by Windows Update, please verify that the following registry key exists and your antivirus software is up to date. Otherwise Windows Update will return no available patches while the system remains vulnerable.

Key="HKEY_LOCAL_MACHINE"Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompa

Value Name="cadca5fe-87d3-4b96-b7fb-a231484277cc"
Type="REG_DWORD”
Data="0x00000000”

Microsoft has issued this guidance to all antivirus vendors, that they must set this registry key to signal to Windows Update that they are compatible with the latest 2018 updates. Please contact your antivirus vendor, or install Windows Defender on the affected system to resolve this condition and allow the system to continue receiving normal updates.

Vulnerability Details

Microsoft has released a security update for Microsoft .NET Framework which includes fixes for the following vulnerabilities:

CVE-2018-0784 - ASP.NET Core Elevation Of Privilege Vulnerability
CVE-2018-0786 - .NET Security Feature Bypass Vulnerability
CVE-2018-0764 - .NET and .NET Core Denial Of Service Vulnerability
CVE-2018-0785 - ASP.NET Core Cross Site Request Forgery Vulnerabilty

Affected Products:
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.5.2 on Windows RT 8.1
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 R2
ASP.NET Core 2.0
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
.NET Core 1.1
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2

Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)
.NET Core 2.0
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft .NET Framework 4.7.1 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for 32-bit Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.7.1 on Windows Server, version 1709 (Server Core Installation)
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.7.1 on Windows 10 Version 1709 for x64-based Systems
Microsoft .NET Framework 4.7 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows Server 2016
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows Server 2012 R2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft .NET Framework 4.6.2/4.7 on Windows Server 2016
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.6 on Windows 10 for x64-based Systems
.NET Core 1.0
Microsoft .NET Framework 3.5 on Windows Server, version 1709 (Server Core Installation)
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.6.1 on Windows 10 Version 1511 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems

Microsoft .NET Framework 3.5 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows 10 Version 1511 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7 on Windows RT 8.1
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems
ASP.NET Core 2.0 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.6.2/4.7 on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0764
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0785
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0784
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0786
BUGTRAQ	http://www.securityfocus.com/bid/102380
BUGTRAQ	http://www.securityfocus.com/bid/102387
BUGTRAQ	http://www.securityfocus.com/bid/102379
BUGTRAQ	http://www.securityfocus.com/bid/102377
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0786
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0764
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0785
URL	https://cwe.mitre.org/data/definitions/352.html

Type	Reference
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://support.microsoft.com/en-us/help/4056891
URL	https://support.microsoft.com/en-us/help/4056888
URL	https://support.microsoft.com/en-us/help/4056890
URL	https://support.microsoft.com/en-us/help/4056892
URL	https://support.microsoft.com/en-us/help/4056893
URL	https://support.microsoft.com/en-us/help/4054996
URL	https://support.microsoft.com/en-us/help/4054998
URL	https://support.microsoft.com/en-us/help/4055000
URL	https://support.microsoft.com/en-us/help/4054994
URL	https://support.microsoft.com/en-us/help/4054172
URL	https://support.microsoft.com/en-us/help/4054176
URL	https://support.microsoft.com/en-us/help/4054993
URL	https://support.microsoft.com/en-us/help/4054182
URL	https://support.microsoft.com/en-us/help/4054177
URL	https://support.microsoft.com/en-us/help/4055002
URL	https://support.microsoft.com/en-us/help/4054181
URL	https://support.microsoft.com/en-us/help/4054999
URL	https://support.microsoft.com/en-us/help/4054175
URL	https://support.microsoft.com/en-us/help/4054183
URL	https://support.microsoft.com/en-us/help/4055001
URL	https://support.microsoft.com/en-us/help/4054174
URL	https://support.microsoft.com/en-us/help/4054995

Type	Reference
URL	https://support.microsoft.com/en-us/help/4054171
URL	https://support.microsoft.com/en-us/help/4054997
URL	https://support.microsoft.com/en-us/help/4054170
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0784

MS18-JAN: Microsoft Windows Security Update (MELTDOWN) Medium

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft Windows which include fixes for the recently released CPU vulnerability known as MELTDOWN and the following vulnerabilities:

CVE-2017-5754 - Meltdown CPU Issue
CVE-2018-0818 - Scripting Engine Security Feature Bypass
CVE-2018-0746 - Windows Information Disclosure Vulnerability
CVE-2018-0747 - Windows Information Disclosure Vulnerability
CVE-2018-0748 - Windows Elevation of Privilege Vulnerability
CVE-2018-0751 - Windows Elevation of Privilege Vulnerability
CVE-2018-0752 - Windows Elevation of Privilege Vulnerability
CVE-2018-0753 - Windows IPSec Denial of Service Vulnerability
CVE-2018-0750 - Windows GDI Information Disclosure Vulnerability
CVE-2018-0788 - OpenType Font Driver Elevation of Privilege Vulnerability
CVE-2018-0741 - Microsoft Color Management Information Disclosure Vulnerability
CVE-2018-0743 - Windows Subsystem for Linux Elevation of Privilege Vulnerability
CVE-2018-0744 - Windows Elevation of Privilege Vulnerability
CVE-2018-0745 - Windows Information Disclosure Vulnerability
CVE-2018-0749 - SMB Server Elevation of Privilege Vulnerability
CVE-2018-0754 - OpenType Font Driver Information Disclosure Vulnerability

Meltdown (CVE-2017-5754) can be leveraged by a malicious program running on the local system to read memory from other processes, including the operating system. Additionally, it may be possible for a malicious program running inside a virtual machine to read memory from the host operating system. This can result in the disclosure of sensitive information which may lead to further compromise.

Affected Products:
Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
Windows 10 Version 1511 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 for 32-bit Systems
Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2
Windows Server 2012 (Server Core installation)

Windows 10 Version 1607 for x64-based Systems
Windows Server 2008 for Itanium-Based Systems Service Pack 2
Windows Server 2016 (Server Core installation)
Windows 10 Version 1511 for 32-bit Systems
Windows 10 Version 1709 for 32-bit Systems
Windows Server 2012
Windows 7 for x64-based Systems Service Pack 1
Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
Windows 7 for 32-bit Systems Service Pack 1
Windows Server 2008 R2 for x64-based Systems Service Pack 1
Windows Server 2008 for x64-based Systems Service Pack 2
Windows 10 Version 1703 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1703 for x64-based Systems
Windows Server 2012 R2 (Server Core installation)
Windows 10 Version 1709 for x64-based Systems
Windows 8.1 for x64-based systems
Windows Server 2012 R2
Windows Server 2016
Windows 8.1 for 32-bit systems
Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Windows Server, version 1709 (Server Core Installation)

Solution Details

Microsoft has released a fix for this flaw in their January 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

PLEASE NOTE: If this patch is not being offered by Windows Update please verify that the following registry key exists and your antivirus software is up to date. Otherwise Windows Update will return no available patches while the system remains vulnerable.

Key="HKEY_LOCAL_MACHINE"Subkey="SOFTWARE\Microsoft\Windows\CurrentVersion\QualityCompa

Value Name="cadca5fe-87d3-4b96-b7fb-a231484277cc"
Type="REG_DWORD”
Data="0x00000000”

Microsoft has issued this guidance to all antivirus vendors, that they must set this registry key to signal to Windows Update that they are compatible with the latest 2018 updates. Please contact your antivirus vendor, or install Windows Defender on the affected system to resolve this condition and allow the system to continue receiving normal updates.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0749
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0818
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0741
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0745
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0788
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0752
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0753
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0751
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0754
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0748
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0750
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0743
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5754
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0744
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0747
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0746
BUGTRAQ	http://www.securityfocus.com/bid/106128
BUGTRAQ	http://www.securityfocus.com/bid/102412
URL	https://support.microsoft.com/en-us/help/4056890
URL	https://support.microsoft.com/en-us/help/4056888
URL	https://support.microsoft.com/en-us/help/4056891
URL	https://support.microsoft.com/en-us/help/4056944
URL	https://www.codeaurora.org/security-bulletin/2018/07/02/july-2018-code-aurora-security-bulletin
URL	https://support.microsoft.com/en-us/help/4056613

Type	Reference
URL	https://support.microsoft.com/en-us/help/4056942
URL	https://support.microsoft.com/en-us/help/4056759
URL	https://source.android.com/security/bulletin/2018-04-01
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cert.vde.com/en-us/advisories/vde-2018-003
URL	https://cert.vde.com/en-us/advisories/vde-2018-002
URL	https://support.citrix.com/article/CTX234679
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03871en_us
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
URL	https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html
URL	https://support.f5.com/csp/article/K91229003
URL	https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-18-0001
URL	https://support.lenovo.com/us/en/solutions/LEN-18282
URL	https://github.com/saaramar/execve_exploit
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://help.ecostruxureit.com/display/public/UADCO8x/StruxureWare+Data+Center+Operation+Software+Vulnerability+Fixes
URL	https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0818
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0741

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0745
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0788
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0752
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0750
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0753
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0751
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0754
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0748
URL	https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-hpesbhf03805en_us
URL	https://support.citrix.com/article/CTX231399
URL	https://security.netapp.com/advisory/ntap-20180104-0001/
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4614
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4613
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0743
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4609
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4611
URL	http://xenbits.xen.org/xsa/advisory-254.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0746
URL	https://01.org/security/advisories/intel-oss-10003

Type	Reference
URL	https://www.synology.com/support/security/Synology_SA_18_01
URL	https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0749
URL	https://95cnsec.com/windows-smb-cve-2018-0749-exploit.html
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0744
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0747
URL	https://access.redhat.com/security/vulnerabilities/speculativeexecution
URL	https://aws.amazon.com/de/security/security-bulletins/AWS-2018-013/
URL	https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/
URL	https://developer.arm.com/support/security-update
URL	https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html
URL	https://meltdownattack.com/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002
URL	https://support.microsoft.com/en-us/help/4056899
URL	https://support.microsoft.com/en-us/help/4056941
URL	https://support.microsoft.com/en-us/help/4056615
URL	https://support.microsoft.com/en-us/help/4056897
URL	https://support.microsoft.com/en-us/help/4056898
URL	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2018-001.txt
URL	https://support.microsoft.com/en-us/help/4056893
URL	https://support.microsoft.com/en-us/help/4056892

MS18-JAN: Microsoft Windows Security Update - Registry Entry Not Set	Medium

Solution Details

The MS18-JAN patch has already been applied. For full remediation of these vulnerabilities, three registry entries need to be created and set to a specific value depending on which processor is used for this asset.

For Intel processors, the following key and values need to be set:

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
Value: FeatureSettingsOverride = 0
Value Type: DWORD (decimal value)

For AMD processors, the following key and values need to be set:

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
Value: FeatureSettingsOverride = 64
Value Type: DWORD (decimal value)

For both Intel and AMD processors, the following key and values need to be set:

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
Value: FeatureSettingsOverrideMask = 3
Value Type: DWORD (decimal value)

If Microsoft Hyper-V is enabled, both Intel and AMD based Windows Servers also require the following key to be set, in addition to the above two keys for the respective CPU:

Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization
Value: MinVmVersionForCpuBasedMitigations = 1.0
Value Type: String Value (REG_SZ)

Example:
For an Intel processor, if the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management doesn't exist, it will first need to be created. After creating it, you'll need to create a new value under this new registry key with the name "FeatureSettingsOverride" (without quotes) that is of type DWORD and set to 0 decimal value.

If the registry key and "FeatureSettingsOverride" already exists, verify that the value is set to 0 decimal value.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Microsoft is aware of a new publicly disclosed class of vulnerabilities referred to as "speculative execution side-channel attacks" that affect many modern processors and operating systems including Intel, AMD, and ARM.

The Microsoft patch for this vulnerability has already been installed, however, the scanner has detected the registry changes required to fully remediate these vulnerabilities have not been set.
Impact:
An attacker who successfully exploited these vulnerabilities may be able to read privileged data across trust boundaries. In shared resource environments (such as exists in some cloud services configurations), these vulnerabilities could allow one virtual machine to improperly access information from another. In non-browsing scenarios on standalone systems, an attacker would need prior access to the system or an ability to run code on the system to leverage these vulnerabilities.

CVSS Base Score: 4.7

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5715
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5753
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5754
BUGTRAQ	http://www.securityfocus.com/bid/106128
BUGTRAQ	http://www.securityfocus.com/bid/102371
BUGTRAQ	http://www.securityfocus.com/bid/102376
URL	https://01.org/security/advisories/intel-oss-10003
URL	https://securityadvisories.paloaltonetworks.com/Home/Detail/121
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
URL	https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability

Type	Reference
URL	https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00088&languageid=en-fr
URL	http://packetstormsecurity.com/files/145645/Spectre-Information-Disclosure-Proof-Of-Concept.html
URL	http://www.arubanetworks.com/assets/alert/ARUBA-PSA-2018-001.txt
URL	https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-18-0001
URL	https://www.vmware.com/security/advisories/VMSA-2018-0007.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
URL	https://spectreattack.com/
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-505225.pdf
URL	https://www.vmware.com/us/security/advisories/VMSA-2018-0002.html
URL	https://www.vmware.com/us/security/advisories/VMSA-2018-0004.html
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4609
URL	http://xenbits.xen.org/xsa/advisory-254.html
URL	https://help.ecostruxureit.com/display/public/UADCO8x/StruxureWare+Data+Center+Operation+Software+Vulnerability+Fixes
URL	https://access.redhat.com/security/vulnerabilities/speculativeexecution
URL	https://aws.amazon.com/de/security/security-bulletins/AWS-2018-013/
URL	https://blog.mozilla.org/security/2018/01/03/mitigations-landing-new-class-timing-attack/
URL	https://developer.arm.com/support/security-update
URL	https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html
URL	https://meltdownattack.com/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002

Type	Reference
URL	https://security.googleblog.com/2018/01/todays-cpu-vulnerability-what-you-need.html
URL	https://support.f5.com/csp/article/K91229003
URL	https://support.lenovo.com/us/en/solutions/LEN-18282
URL	https://www.suse.com/c/suse-addresses-meltdown-spectre-vulnerabilities/
URL	https://www.synology.com/support/security/Synology_SA_18_01
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4611
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4613
URL	http://nvidia.custhelp.com/app/answers/detail/a_id/4614
URL	https://security.netapp.com/advisory/ntap-20180104-0001/
URL	https://support.citrix.com/article/CTX231399
URL	https://support.hpe.com/hpsc/doc/public/display?docId=emr_na-hpesbhf03805en_us
URL	https://support.microsoft.com/en-us/help/4072698/windows-server-speculative-execution-side-channel-v
URL	https://source.android.com/security/bulletin/2018-04-01
URL	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
URL	https://www.codeaurora.org/security-bulletin/2018/07/02/july-2018-code-aurora-security-bulletin
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
URL	https://cert.vde.com/en-us/advisories/vde-2018-003
URL	https://support.citrix.com/article/CTX234679
URL	https://cert.vde.com/en-us/advisories/vde-2018-002

Type	Reference
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03871en_us
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-

MS18-JUL: Microsoft .NET Security Update

Medium

Vulnerability Details

Microsoft has released a security update for Microsoft .NET Framework which includes fixes for the following vulnerabilities:

CVE-2018-8202 - .NET Framework Elevation of Privilege Vulnerability
CVE-2018-8356 - .NET Framework Security Feature Bypass Vulnerability
CVE-2018-8260 - .NET Framework Remote Code Execution Vulnerability
CVE-2018-8284 - .NET Framework Remote Code Injection Vulnerability
CVE-2018-8171 - ASP.NET Security Feature Bypass Vulnerability

Affected Products:
ASP.NET Core 1.1
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for 32-bit Systems
ASP.NET Web Pages 3.2.3 on Microsoft Visual Studio 2013 Update 5
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.5.2 on Windows RT 8.1
Microsoft .NET Framework 4.7.2 on Windows Server 2016
Microsoft .NET Framework 4.7.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems
Microsoft .NET Framework 4.7.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 4.7.2 on Windows Server, version 1803 (Server Core Installation)
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2
ASP.NET Core 2.0
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
.NET Core 1.1
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1

ASP.NET MVC 5.2 on Microsoft Visual Studio 2015 Update 3
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.7.2 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems
Microsoft .NET Framework 4.7.2 on Windows Server 2012
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft .NET Framework 4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for x64-based Systems
.NET Core 2.0
Microsoft .NET Framework 4.7.1/4.7.2 on Windows Server, version 1709 (Server Core Installation)
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for 32-bit Systems
ASP.NET Web Pages 3.2.3 on Microsoft Visual Studio 2015 Update 3
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1709 for x64-based Systems
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
.NET Framework 4.7.2 Developer Pack
Microsoft .NET Framework 3.5 on Windows Server 2016
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows RT 8.1
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows Server 2012 R2
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1

Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2
Microsoft .NET Framework 4.7.2 on Windows Server 2012 R2
Microsoft .NET Framework 4.7.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.7.2 on Windows Server, version 1709 (Server Core Installation)
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.7.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
ASP.NET Core 1.0
.NET Core 1.0
Microsoft .NET Framework 3.5 on Windows Server, version 1709 (Server Core Installation)
ASP.NET MVC 5.2 on Microsoft Visual Studio 2013 Update 5
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 4.7.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows Server 2012
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows Server 2012
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows Server 2012 R2
Microsoft .NET Framework 4.7.2 on Windows RT 8.1
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for x64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.7.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for 32-bit Systems

Solution Details

Microsoft has released a fix for this flaw in their July 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8284
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8260
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8356
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8171
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8202
BUGTRAQ	http://www.securityfocus.com/bid/104666
BUGTRAQ	http://www.securityfocus.com/bid/104665
BUGTRAQ	http://www.securityfocus.com/bid/104659
BUGTRAQ	http://www.securityfocus.com/bid/104667
URL	https://support.microsoft.com/en-us/help/4338829
URL	https://support.microsoft.com/en-us/help/4338423
URL	https://support.microsoft.com/en-us/help/4338601
URL	https://support.microsoft.com/en-us/help/4338416
URL	https://support.microsoft.com/en-us/help/4338415
URL	https://support.microsoft.com/en-us/help/4338422
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.microsoft.com/en-us/help/4338610
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8260
URL	https://support.microsoft.com/en-us/help/4338814
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8202

Type	Reference
URL	https://support.microsoft.com/en-us/help/4338417
URL	https://support.microsoft.com/en-us/help/4338602
URL	https://support.microsoft.com/en-us/help/4338420
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8284
URL	https://support.microsoft.com/en-us/help/4338819
URL	https://support.microsoft.com/en-us/help/4338613
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8356
URL	https://support.microsoft.com/en-us/help/4338605
URL	https://support.microsoft.com/en-us/help/4338604
URL	https://support.microsoft.com/en-us/help/4338612
URL	https://support.microsoft.com/en-us/help/4338421
URL	https://support.microsoft.com/en-us/help/4339279
URL	https://support.microsoft.com/en-us/help/4338418
URL	https://support.microsoft.com/en-us/help/4338611
URL	https://support.microsoft.com/en-us/help/4338424
URL	https://support.microsoft.com/en-us/help/4338600
URL	https://support.microsoft.com/en-us/help/4338826
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8171
URL	https://cwe.mitre.org/data/definitions/295.html
URL	https://support.microsoft.com/en-us/help/4338825
URL	https://support.microsoft.com/en-us/help/4338606
URL	https://support.microsoft.com/en-us/help/4338419

MS18-MAY: Microsoft .NET Security Update | Medium

Vulnerability Details

Microsoft has released a security update for Microsoft .NET Framework which includes fixes for the following vulnerabilities:

CVE-2018-1039 - .NET Framework Device Guard Security Feature Bypass Vulnerability
CVE-2018-0765 - .NET and .NET Core Denial of Service Vulnerability

Affected Products:
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.7/4.7.1 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 4.6.2/4.7/4.7.1 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.5.2 on Windows RT 8.1
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6.2/4.7/4.7.1 on Windows Server 2016
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows Server 2012
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.7.2 on Windows Server, version 1803 (Server Core Installation)
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1/4.6.2 on Windows 10 for x64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows 8.1 for 32-bit systems
.NET Core 2.0
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft .NET Framework 4.7.1 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2

Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows Server 2012 R2
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows RT 8.1
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.7.1 on Windows Server, version 1709 (Server Core Installation)
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.7/4.7.1 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.7.1 on Windows 10 Version 1709 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows Server 2016
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows Server 2012 R2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows Server, version 1709 (Server Core Installation)
Microsoft .NET Framework 4.6.2/4.7/4.7.1 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 4.6.2/4.7/4.7.1 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for 32-bit Systems

Solution Details

Microsoft has released a fix for this flaw in their May 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-0765
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1039
BUGTRAQ	http://www.securityfocus.com/bid/104072
BUGTRAQ	http://www.securityfocus.com/bid/104060
URL	https://support.microsoft.com/en-us/help/4096236
URL	https://support.microsoft.com/en-us/help/4095514
URL	https://support.microsoft.com/en-us/help/4096416
URL	https://support.microsoft.com/en-us/help/4095517
URL	https://support.microsoft.com/en-us/help/4096418
URL	https://support.microsoft.com/en-us/help/4096417
URL	https://support.microsoft.com/en-us/help/4103721
URL	https://support.microsoft.com/en-us/help/4095872
URL	https://support.microsoft.com/en-us/help/4096494
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-0765
URL	https://support.microsoft.com/en-us/help/4096235
URL	https://support.microsoft.com/en-us/help/4096237
URL	https://support.microsoft.com/en-us/help/4095518
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-1039
URL	https://support.microsoft.com/en-us/help/4103716
URL	https://support.microsoft.com/en-us/help/4103723

Type	Reference
URL	https://cwe.mitre.org/data/definitions/611.html
URL	https://support.microsoft.com/en-us/help/4095875
URL	https://support.microsoft.com/en-us/help/4095873
URL	https://support.microsoft.com/en-us/help/4095513
URL	https://support.microsoft.com/en-us/help/4095512
URL	https://support.microsoft.com/en-us/help/4095876
URL	https://support.microsoft.com/en-us/help/4095874
URL	https://support.microsoft.com/en-us/help/4103727
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://support.microsoft.com/en-us/help/4095515
URL	https://support.microsoft.com/en-us/help/4096495
URL	https://support.microsoft.com/en-us/help/4103731
URL	https://support.microsoft.com/en-us/help/4095519

MS18-NOV: Microsoft Internet Explorer Security Update — Medium

Solution Details

Microsoft has released a fix for this flaw in their November 2018 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2018-8552 - Windows Scripting Engine Memory Corruption Vulnerability
CVE-2018-8570 - Internet Explorer Memory Corruption Vulnerability

Affected Products:
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for x64-based systems

Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems
Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8552
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-8570
BUGTRAQ	http://www.securityfocus.com/bid/105783
BUGTRAQ	http://www.securityfocus.com/bid/105786
URL	https://support.microsoft.com/en-us/help/4467708
URL	https://support.microsoft.com/en-us/help/4467702
URL	https://support.microsoft.com/en-us/help/4467701
URL	https://support.microsoft.com/en-us/help/4466536
URL	https://support.microsoft.com/en-us/help/4467691

Type	Reference
URL	https://support.microsoft.com/en-us/help/4467706
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8552
URL	https://support.microsoft.com/en-us/help/4467107
URL	https://support.microsoft.com/en-us/help/4467680
URL	https://support.microsoft.com/en-us/help/4467686
URL	https://support.microsoft.com/en-us/help/4467697
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2018-8570
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4467696

MS18-NOV: Microsoft Windows Security Update - Registry Entry Not Set

Medium

Solution Details

The MS18-NOV patch has already been applied. For full remediation of this vulnerability, three registry entries need to be created and set to a specific value depending on which processor is used for this asset.

The registry values are different depending on processor architecture.

For Intel processors, the following key and values need to be set:
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
Value: FeatureSettingsOverride = 8
Value Type: DWORD (decimal value)

For AMD processors, the following key and values need to be set:
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
Value: FeatureSettingsOverride = 72
Value Type: DWORD (decimal value)

For both Intel and AMD processors, the following key and values need to be set:
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory

Management
Value: FeatureSettingsOverrideMask = 3
Value Type: DWORD (decimal value)

If Microsoft Hyper-V is enabled, both Intel and AMD based Windows Servers also require the following key to be set, in addition to the above two keys for the respective CPU:
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization
Value: MinVmVersionForCpuBasedMitigations = 1.0
Value Type: String Value (REG_SZ)

Example:
For an Intel processor, if the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management doesn't exist, it will first need to be created. After creating it, you'll need to create a new value under this new registry key with the name "FeatureSettingsOverride" (without quotes) that is of type DWORD and set to 8 decimal value.

If the registry key and "FeatureSettingsOverride" already exists, verify that the value is set to 8 decimal value.

Vulnerability Details

On January 3, 2018, Microsoft released an advisory and security updates related to a newly-discovered class of hardware vulnerabilities (known as Spectre and Meltdown) involving speculative execution side channels. A new subclass of speculative execution side channel vulnerabilities known as Speculative Store Bypass (SSB) has been announced and assigned CVE-2018-3639.

The Microsoft patch for this vulnerability has already been installed, however, the scanner has detected the registry changes required to fully remediate this vulnerability have not been set.
Impact:
An attacker who has successfully exploited this vulnerability may be able to read privileged data across trust boundaries.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.1

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-3639
BUGTRAQ	http://www.securityfocus.com/bid/104232
URL	http://support.lenovo.com/us/en/solutions/LEN-22133

Type	Reference
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://security.netapp.com/advisory/ntap-20180521-0001/
URL	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html
URL	https://www.synology.com/support/security/Synology_SA_18_23
URL	http://xenbits.xen.org/xsa/advisory-263.html
URL	https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-
URL	https://bugs.chromium.org/p/project-zero/issues/detail?id=1528
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180012
URL	https://support.citrix.com/article/CTX235225
URL	http://www.fujitsu.com/global/support/products/software/security/products-f/cve-2018-3639e.html
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-505225.pdf
URL	https://nvidia.custhelp.com/app/answers/detail/a_id/4787
URL	https://support.oracle.com/knowledge/Sun%20Microsystems/2481872_1.html
URL	https://support.microsoft.com/en-us/help/4072698/windows-server-speculative-execution-side-channel-v
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03850en_us
URL	https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-18-0006
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-268644.pdf
URL	https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability
URL	https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0004

MS19-JAN: Microsoft Internet Explorer Security Update — Medium

Vulnerability Details

Microsoft has released cumulative security updates for Internet Explorer which include fixes for the following vulnerabilities:

CVE-2019-0541 - MSHTML Engine Remote Code Execution Vulnerability

Affected Products:
Microsoft Office 2010 Service Pack 2 (64-bit editions)
Internet Explorer 11 on Windows 10 Version 1703 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1703 for 32-bit Systems
Microsoft Office 2016 (32-bit edition)
Internet Explorer 11 on Windows 8.1 for x64-based systems
Internet Explorer 11 on Windows 10 Version 1709 for 32-bit Systems
Internet Explorer 11 on Windows 10 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for 32-bit Systems
Microsoft Office 2016 (64-bit edition)
Internet Explorer 11 on Windows 10 Version 1709 for ARM64-based Systems
Internet Explorer 11 on Windows 10 Version 1803 for ARM64-based Systems
Internet Explorer 9 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft Office 2010 Service Pack 2 (32-bit editions)
Internet Explorer 11 on Windows 10 Version 1709 for x64-based Systems
Microsoft Excel Viewer 2007 Service Pack 3
Microsoft Office Word Viewer
Internet Explorer 11 on Windows Server 2019
Internet Explorer 11 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft Office 2019 for 32-bit editions
Office 365 ProPlus for 64-bit Systems
Internet Explorer 11 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Internet Explorer 11 on Windows Server 2016
Internet Explorer 11 on Windows 10 Version 1803 for 32-bit Systems
Internet Explorer 11 on Windows 10 Version 1607 for x64-based Systems
Microsoft Office 2013 Service Pack 1 (32-bit editions)
Microsoft Office 2019 for 64-bit editions
Internet Explorer 10 on Windows Server 2012
Internet Explorer 11 on Windows 7 for 32-bit Systems Service Pack 1
Internet Explorer 11 on Windows 10 Version 1809 for x64-based Systems
Microsoft Office 2013 Service Pack 1 (64-bit editions)
Internet Explorer 11 on Windows RT 8.1
Internet Explorer 11 on Windows 10 for x64-based Systems
Internet Explorer 11 on Windows 8.1 for 32-bit systems
Internet Explorer 11 on Windows Server 2012 R2
Microsoft Office 2013 RT Service Pack 1
Internet Explorer 11 on Windows 10 Version 1803 for x64-based Systems
Internet Explorer 11 on Windows 10 Version 1809 for 32-bit Systems

Internet Explorer 11 on Windows 7 for x64-based Systems Service Pack 1
Office 365 ProPlus for 32-bit Systems
Internet Explorer 9 on Windows Server 2008 for x64-based Systems Service Pack 2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Microsoft has released a fix for this flaw in their January 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

CVSS Base Score: 8.8

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0541
BUGTRAQ	http://www.securityfocus.com/bid/106402
URL	https://support.microsoft.com/en-us/help/4480965
URL	https://support.microsoft.com/en-us/help/4480970
URL	https://support.microsoft.com/en-us/help/4480961
URL	https://support.microsoft.com/en-us/help/3172522
URL	https://support.microsoft.com/en-us/help/4480962
URL	https://support.microsoft.com/en-us/help/4480973
URL	https://support.microsoft.com/en-us/help/4480978
URL	https://support.microsoft.com/en-us/help/2553332
URL	https://support.microsoft.com/en-us/help/4480963
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.microsoft.com/en-us/help/4480975
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0541
URL	https://support.microsoft.com/en-us/help/4480116
URL	https://support.microsoft.com/en-us/help/4480968

Type	Reference
URL	https://support.microsoft.com/en-us/help/4462112
URL	https://support.microsoft.com/en-us/help/4022162
URL	https://support.microsoft.com/en-us/help/4480966
URL	https://support.microsoft.com/en-us/help/2596760

MS19-MAY: Microsoft .NET Security Update — Medium

Solution Details

Microsoft has released a fix for this flaw in their May 2019 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released a security update for Microsoft .NET Framework which includes fixes for the following vulnerabilities:

CVE-2019-0980 - .Net Framework and .Net Core Denial of Service Vulnerability
CVE-2019-0981 - .Net Framework and .Net Core Denial of Service Vulnerability
CVE-2019-0820 - .NET Framework and .NET Core Denial of Service Vulnerability
CVE-2019-0864 - .NET Framework Denial of Service Vulnerability

Affected Products:
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 4.6.2 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.7.2 on Windows Server 2019 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 4.8 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.5.2 on Windows RT 8.1
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for 32-bit Systems
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for x64-based Systems
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for 32-bit Systems
Microsoft .NET Framework 4.7.2 on Windows Server, version 1803 (Server Core Installation)
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for x64-based Systems
.NET Core 1.1
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)

Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows Server, version 1803 (Server Core Installation)
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for ARM64-based Systems
Microsoft .NET Framework 4.8 on Windows Server 2012
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.6.2 on Windows 10 for x64-based Systems
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 4.5.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for x64-based Systems
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for 32-bit Systems
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1903 for x64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for Itanium-Based Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 4.8 on Windows RT 8.1
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for x64-based Systems
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 3.5 on Windows 10 for x64-based Systems
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.7/4.7.1/4.7.2 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 4.8 on Windows 10 Version 1903 for 32-bit Systems
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for 32-bit Systems
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.5.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.8 on Windows 10 Version 1709 for x64-based Systems
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft .NET Framework 3.5 on Windows Server 2016

Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows Server, version 1903 (Server Core installation)
Microsoft .NET Framework 4.5.2 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows Server 2019
Microsoft .NET Framework 4.8 on Windows Server 2016
Microsoft .NET Framework 3.5 on Windows Server, version 1903 (Server Core installation)
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for ARM64-based Systems
Microsoft .NET Framework 3.5 on Windows Server 2012 R2
Microsoft .NET Framework 4.5.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.8 on Windows Server 2019 (Server Core installation)
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
Microsoft .NET Framework 4.5.2 on Windows Server 2012 R2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 4.8 on Windows Server 2019
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.8 on Windows 10 Version 1809 for x64-based Systems
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
.NET Core 1.0
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2
Microsoft .NET Framework 4.8 on Windows Server 2012 R2
.NET Core 2.1
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows 10 Version 1803 for ARM64-based Systems
Microsoft .NET Framework 4.7.1/4.7.2 on Windows 10 Version 1709 for 32-bit Systems
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for 32-bit Systems
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows Server 2019 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows Server 2012
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 4.8 on Windows Server, version 1803 (Server Core Installation)
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
.NET Core 2.2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for x64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack

1
Microsoft .NET Framework 3.5 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 10 Version 1703 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1809 for x64-based Systems
Microsoft .NET Framework 4.7.2 on Windows Server 2019
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 3.5 on Windows 10 for 32-bit Systems
Microsoft .NET Framework 4.8 on Windows 10 Version 1803 for x64-based Systems
Microsoft .NET Framework 3.5 on Windows 10 Version 1709 for ARM64-based Systems
Microsoft .NET Framework 4.7.2 on Windows 10 Version 1803 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.5

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0864
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0981
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0980
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-0820
URL	https://support.microsoft.com/en-us/help/4498962
URL	https://support.microsoft.com/en-us/help/4495610
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0820
URL	https://support.microsoft.com/en-us/help/4498961
URL	https://support.microsoft.com/en-us/help/4499407
URL	https://support.microsoft.com/en-us/help/4495620
URL	https://support.microsoft.com/en-us/help/4499406
URL	https://support.microsoft.com/en-us/help/4499405
URL	https://support.microsoft.com/en-us/help/4499408

Type	Reference
URL	https://support.microsoft.com/en-us/help/4499409
URL	https://support.microsoft.com/en-us/help/4495616
URL	https://support.microsoft.com/en-us/help/4498964
URL	https://support.microsoft.com/en-us/help/4495611
URL	https://support.microsoft.com/en-us/help/4498963
URL	https://support.microsoft.com/en-us/help/4495613
URL	https://cwe.mitre.org/data/definitions/19.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://support.microsoft.com/en-us/help/4499179
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://support.microsoft.com/en-us/help/4499181
URL	https://support.microsoft.com/en-us/help/4494440
URL	https://support.microsoft.com/en-us/help/4499167
URL	https://support.microsoft.com/en-us/help/4499154
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0980
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0864
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0981

MS19-MAY: Microsoft Windows Security Update (ZombieLoad) - Registry Entry Not Set

Medium

Solution Details

The MS19-MAY patch has already been applied. For full remediation of this vulnerability, multiple registry entries need to be created and set to a specific value depending if the asset is a client or server machine and if hyper-threading is enabled or not. Note, these changes only need to be made for hosts using a 64 bit Intel processor. AMD and 32 bit Intel processors aren't vulnerable.

With hyper-threading enabled: (for both servers and clients)
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
Value: FeatureSettingsOverride = 72
Value Type: DWORD (decimal value)

With hyper-threading disabled: (for both servers and clients)
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
Value: FeatureSettingsOverride = 8264
Value Type: DWORD (decimal value)

This value is the same regardless of hyper-threading or type of machine (servers or clients)
Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
Value: FeatureSettingsOverrideMask = 3
Value Type: DWORD (decimal value)

This key/value is only required for machines with Microsoft Hyper-V enabled:
Key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Virtualization
Value: MinVmVersionForCpuBasedMitigations = 1.0
Value Type: String Value (REG_SZ)

Example:
For a host with hyper-threading disabled, if the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management doesn't exist, it will first need to be created. After creating it, you'll need to create a new value under this new registry key with the name "FeatureSettingsOverride" (without quotes) that is of type DWORD and set to 8264 decimal value.

If the registry key and "FeatureSettingsOverride" already exists and hyper-threading is disabled, verify that the value is set to 8264 decimal value.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

On January 3, 2018, Microsoft released an advisory and security updates related to a newly-discovered class of hardware vulnerabilities (known as Spectre and Meltdown) involving speculative execution side channels. A new subclass of speculative execution side channel vulnerabilities known as Microarchitectural Data Sampling has been announced.

The Microsoft patch for this vulnerability has already been installed, however, the scanner has detected the registry changes required to fully remediate this vulnerability have not been set.
Impact:
An attacker who has successfully exploited this vulnerability may be able to read privileged data across trust boundaries.

CVSS Base Score: 4.7

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12127
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12126
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-11091
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12130
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://support.microsoft.com/en-us/help/4072698/windows-server-speculative-execution-side-channel-v
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV190013
URL	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html

MS19-NOV: Microsoft Windows Security Update - Registry Entry Not Set

Medium

Solution Details

The MS19-NOV patch has already been applied. By default, all Windows client operating systems and Windows Server 2019 have the mitigation for this vulnerability enabled. However, the earlier Windows Server versions do not have this mitigation enabled by default. In order to fully remediate this vulnerability on the earlier versions of Windows server, a registry entry needs to be added. Additionally, this vulnerability only affects Intel processors.

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Kernel
Value: DisableTsx = 1
Value Type: DWORD (Decimal value)

Vulnerability Details

An information disclosure vulnerability exists when the Windows kernel improperly handles objects in memory. To exploit this vulnerability, an attacker would have to log on to an affected system and run a specially crafted application. The vulnerability would not allow an attacker to execute code or to elevate user rights directly, but it could be used to obtain information that could be used to try to further compromise the affected system.

The Microsoft patch for this vulnerability has already been installed, however, the scanner has detected the registry changes required to fully remediate this vulnerability have not been set.

Impact:
An attacker who successfully exploited this vulnerability could obtain information to further compromise the user’s system.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.1

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-11135
URL	https://support.microsoft.com/en-us/help/4072698/windows-server-speculative-execution-side-channel-v
URL	https://support.microsoft.com/en-us/help/4531006/guidance-for-disabling-intel-transactional-synchron
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-11135
URL	https://support.microsoft.com/en-us/help/4073119/protect-against-speculative-execution-side-channel-

MS21-JAN: Microsoft SQL Server Security Update — Medium

Solution Details

Microsoft has released a fix for this flaw in their January 2021 Security Update. Please download and install the patch from the Microsoft Update Catalog.

Vulnerability Details

Microsoft has released cumulative security updates for Microsoft SQL Server which include fixes for the following vulnerabilities:

CVE-2021-1636 - Microsoft SQL Elevation of Privilege Vulnerability

Affected Products:
Microsoft SQL Server 2016 for x64-based Systems Service Pack 2 (GDR)
Microsoft SQL Server 2012 for x64-based Systems Service Pack 4 (QFE)
Microsoft SQL Server 2017 for x64-based Systems (CU 22)
Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (GDR)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (CU 4)
Microsoft SQL Server 2012 for 32-bit Systems Service Pack 4 (QFE)
Microsoft SQL Server 2017 for x64-based Systems (GDR)

Microsoft SQL Server 2014 Service Pack 3 for x64-based Systems (CU 4)
Microsoft SQL Server 2019 for x64-based Systems (GDR)
Microsoft SQL Server 2016 Service Pack 2 for x64-based Systems (CU 15)
Microsoft SQL Server 2019 for x64-based Systems (CU 8)
Microsoft SQL Server 2014 Service Pack 3 for 32-bit Systems (GDR)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.5

CVSS Vector: AV:N/AC:L/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-1636
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1636
URL	https://support.microsoft.com/en-us/help/4583462
URL	https://support.microsoft.com/en-us/help/4583456
URL	https://support.microsoft.com/en-us/help/4583459
URL	https://support.microsoft.com/en-us/help/4583458
URL	https://support.microsoft.com/en-us/help/4583460
URL	https://support.microsoft.com/en-us/help/4583465
URL	https://support.microsoft.com/en-us/help/4583461
URL	https://support.microsoft.com/en-us/help/4583457
URL	https://support.microsoft.com/en-us/help/4583463

NetBIOS Shares Accessible — Medium

Solution Details

Review the shares that are listed in the vulnerability data section. Disable any shares that are unnecessary.

On Microsoft Windows operating systems, the shares on the local or remote machines can be viewed by using the "Shared Folders" Snap-in of the Microsoft Management Console (MMC). There are three shares that are present by default and cannot be modified: ADMIN$, C$, IPC$. All other shares should be listed and modifiable through this Snap-in.

For Samba installations, modify the smb.conf file so that it either specifies the users who are allowed to access the host in the 'valid users' field, or so that it specifies the allowed hosts in the 'hosts allow' field. The smb.conf file is typically found in the /etc/samba/ directory but this location varies between system distributions.

Note: Specific UNIX distributions may require different steps. Please consult the Samba documentation for further details.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This host revealed one or more NetBIOS shares that did not require any authentication to access. An attacker can read data from these NetBIOS shares or potentially trojan files in an effort to compromise this host.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519
URL	http://support.microsoft.com/kb/314984

OpenSSH Account Enumeration Vulnerability — Medium

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

Vulnerability Details

OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-2768

OpenSSH 'auth-gss2.c' User Detection Vulnerability — Medium

Vulnerability Details

Remotely observable behaviour in auth-gss2.c in OpenSSH through 7.8 could be used by remote attackers to detect existence of users on a target system when GSS2 is in use. NOTE: the discoverer states 'We understand that the OpenSSH developers do not want to treat such a username enumeration (or "oracle") as a vulnerability.'
Impact:
An attacker may leverage this issue to harvest valid user accounts, which may aid in brute-force attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

CVSS Base Score: 5.3

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-15919
BUGTRAQ	http://www.securityfocus.com/bid/105163
URL	http://seclists.org/oss-sec/2018/q3/180
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://security.netapp.com/advisory/ntap-20181221-0001/

OpenSSH 'before 7.6' 'process_open function in sftp-server.c' subcomponent Does not Properly Prevent Write Operations in Readonly Mode Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15906
BUGTRAQ	http://www.securityfocus.com/bid/101552
URL	https://security.netapp.com/advisory/ntap-20180423-0004/
URL	https://cwe.mitre.org/data/definitions/275.html
URL	https://www.openssh.com/txt/release-7.6
URL	https://github.com/openbsd/src/commit/a6981567e8e215acc1ef690c8dbb30f2d9b00a19

OpenSSH BLOWFISH Hashing User Enumeration — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6210
BUGTRAQ	http://www.securityfocus.com/bid/91812

Type	Reference
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://security.netapp.com/advisory/ntap-20190206-0001/
URL	https://www.openssh.com/txt/release-7.3

OpenSSH Heap-Based Buffer Overflow Vulnerability — Medium

Vulnerability Details

The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

CVSS Base Score: 4.6

CVSS Vector: AV:N/AC:H/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0778
BUGTRAQ	http://www.securityfocus.com/bid/80698
URL	http://packetstormsecurity.com/files/135273/Qualys-Security-Advisory-OpenSSH-Overflow-Leak.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680
URL	http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html
URL	http://www.openssh.com/txt/release-7.1p2

Type	Reference
URL	https://bto.bluecoat.com/security-advisory/sa109
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10734
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05247375
URL	https://blogs.sophos.com/2016/02/29/utm-up2date-9-319-released/
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://support.apple.com/HT206167
URL	https://blogs.sophos.com/2016/02/17/utm-up2date-9-354-released/

OpenSSH Information Disclosure Vulnerability — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

Vulnerability Details

The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

CVSS Base Score: 4

CVSS Vector: AV:N/AC:L/Au:S/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-0777
BUGTRAQ	http://www.securityfocus.com/bid/80695
URL	https://blogs.sophos.com/2016/02/17/utm-up2date-9-354-released/
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10734
URL	https://support.apple.com/HT206167

Type	Reference
URL	https://bto.bluecoat.com/security-advisory/sa109
URL	http://packetstormsecurity.com/files/135273/Qualys-Security-Advisory-OpenSSH-Overflow-Leak.html
URL	http://www.openssh.com/txt/release-7.1p2
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://blogs.sophos.com/2016/02/29/utm-up2date-9-319-released/
URL	http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05247375
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722

OpenSSH kex.c and packet.c NULL Pointer Dereference Denial of Service

Medium

Vulnerability Details

sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10708
BUGTRAQ	http://www.securityfocus.com/bid/102780
URL	https://security.netapp.com/advisory/ntap-20180423-0003/
URL	https://www.openssh.com/releasenotes.html
URL	https://cwe.mitre.org/data/definitions/476.html
URL	https://anongit.mindrot.org/openssh.git/commit/?id=28652bca29046f62c7045e933e6b931de1d16737
URL	http://blog.swiecki.net/2018/01/fuzzing-tcp-servers.html
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10284

OpenSSH Missing Character Man-in-The-Middle Attack Vulnerability — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References for a link to upgrade to the most recent stable version of OpenSSH.

Vulnerability Details

An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.
Impact:
Successfully exploiting this issue allows attackers to perform man-in-the-middle attacks and bypass certain security restrictions.

CVSS Base Score: 4

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-6109
URL	https://cwe.mitre.org/data/definitions/284.html

Type	Reference
URL	https://security.netapp.com/advisory/ntap-20190213-0001/
URL	https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt
URL	https://cvsweb.openbsd.org/src/usr.bin/ssh/scp.c
URL	https://www.openssh.com/
URL	https://cvsweb.openbsd.org/src/usr.bin/ssh/progressmeter.c

OpenSSH monitor.c 'mm_answer_pam_free_ctx' Use-After-Free Vulnerability

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.9

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6564
BUGTRAQ	http://www.securityfocus.com/bid/76317
URL	https://github.com/openssh/openssh-portable/commit/5e75f5198769056089fb06c4d738ab0e5abc66f7
URL	https://www.broadcom.com/support/fibre-channel-networking/security-advisories/brocade-security-advisory-2019-764
URL	http://www.openssh.com/txt/release-7.0
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html

Type	Reference
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2016-2867206.html

OpenSSH 'Observable Discrepancy' Man-in-the-Middle Vulnerability — Medium

Solution Details

Update to the most recent stable version of OpenSSH.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The client side in OpenSSH has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).
Impact:
An attacker could leverage this vulnerability to gain access to sensitive information without proper authorization.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-14145

OpenSSH Privilege Escalation Vulnerability — Medium

Vulnerability Details

sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please upgrade to the latest version.

CVSS Base Score: 4.4

CVSS Vector: AV:L/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-41617
URL	https://www.openwall.com/lists/oss-security/2021/09/26/1
URL	https://www.openssh.com/security.html
URL	https://bugzilla.suse.com/show_bug.cgi?id=1190975

OpenSSH Privilege Escalation Vulnerability — Medium

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

Vulnerability Details

sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.9

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10010
BUGTRAQ	http://www.securityfocus.com/bid/94972
URL	https://security.netapp.com/advisory/ntap-20171130-0002/
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03818en_us
URL	https://github.com/openbsd/src/commit/c76fac666ea038753294f2ac94d310f8adece9ce
URL	http://packetstormsecurity.com/files/140262/OpenSSH-Local-Privilege-Escalation.html

Type	Reference
URL	https://bugs.chromium.org/p/project-zero/issues/detail?id=1010
URL	http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.647637
URL	https://www.openssh.com/txt/release-7.4

OpenSSH Remote Command Injection Vulnerability — Medium

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

Vulnerability Details

Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.5

CVSS Vector: AV:N/AC:L/Au:S/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3115
BUGTRAQ	http://www.securityfocus.com/bid/84314
URL	http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/session.c
URL	http://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/session.c.diff?r1=1.281&r2=1.282&f=h
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
URL	http://www.oracle.com/technetwork/topics/security/ovmbulletinjul2016-3090546.html
URL	https://bto.bluecoat.com/security-advisory/sa121
URL	http://packetstormsecurity.com/files/136234/OpenSSH-7.2p1-xauth-Command-Injection-Bypass.html

Type	Reference
URL	https://github.com/tintinweb/pub/tree/master/pocs/cve-2016-3115
URL	http://www.openssh.com/txt/x11fwd.adv

OpenSSH 'scp' Command Evaluation Vulnerability — Medium

Solution Details

Use of rsync in the place of scp for better security. If scp is required, please ensure it is updated with the latest patches and fixes from the vendor.

Vulnerability Details

scp in OpenSSH through 8.3p1 allows command injection in scp.c remote function, as demonstrated by backtick characters in the destination argument.
Impact:
An attacker can exploit this vulnerability to cause a denial-of-service condition, denying service to legitimate users or obtain a reverse shell.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-15778

OpenSSH scp Server Man-in-The-Middle Attack Vulnerability — Medium

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of OpenSSH.

Vulnerability Details

An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).
Impact:
Successfully exploiting this issue allows attackers to perform man-in-the-middle attacks and bypass certain security restrictions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-6111
BUGTRAQ	http://www.securityfocus.com/bid/106741
URL	https://www.openssh.com/
URL	https://security.netapp.com/advisory/ntap-20190213-0001/
URL	https://cvsweb.openbsd.org/src/usr.bin/ssh/scp.c
URL	https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1677794
URL	https://cwe.mitre.org/data/definitions/20.html

OpenSSH Sensitive Data Exposure Vulnerability — Medium

Vulnerability Details

OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session.

Solution Details

Please upgrade to the latest version.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.3

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-20012
URL	https://www.openssh.com/security.html

Type	Reference
URL	https://github.com/openssh/openssh-portable/blob/d0fffc88c8fe90c1815c6f4097bc8cbcabc0f3dd/auth2-pubkey.c#L261-L265
URL	https://github.com/openssh/openssh-portable/pull/270

OpenSSH 'ssh_packet_read_poll2' Function Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The ssh_packet_read_poll2 function in packet.c in OpenSSH before 7.1p2 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted network traffic.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.3

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1907
BUGTRAQ	http://www.securityfocus.com/bid/81293
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://www.openssh.com/txt/release-7.1p2
URL	https://bto.bluecoat.com/security-advisory/sa109
URL	https://anongit.mindrot.org/openssh.git/commit/?id=2fecfd486bdba9f51b3a789277bb0733ca36e1c0
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680

OpenSSH 'stderr' Man-in-The-Middle Attack Vulnerability — Medium

Solution Details

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.
Impact:
Successfully exploiting this issue allows attackers to perform man-in-the-middle attacks and bypass certain security restrictions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-6110
URL	https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt
URL	https://www.openssh.com/
URL	https://cvsweb.openbsd.org/src/usr.bin/ssh/progressmeter.c
URL	https://security.netapp.com/advisory/ntap-20190213-0001/
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://cvsweb.openbsd.org/src/usr.bin/ssh/scp.c

OpenSSH User Enumeration Vulnerability — Medium

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

Vulnerability Details

OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

Impact:
A remote user can determine valid usernames on the target system.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-15473
BUGTRAQ	http://www.securityfocus.com/bid/105140
URL	https://github.com/openbsd/src/commit/779974d35b4859c07bc3cb8a12c74b43b0a7d1e0
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0011
URL	https://security.netapp.com/advisory/ntap-20181101-0001/
URL	https://bugs.debian.org/906236
URL	http://www.openwall.com/lists/oss-security/2018/08/15/5

OpenSSH 'x11_open_helper' Function Access Restriction Bypass — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5352
BUGTRAQ	http://www.securityfocus.com/bid/75525
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2016-2867206.html
URL	http://www.openssh.com/txt/release-6.9
URL	https://anongit.mindrot.org/openssh.git/commit/?h=V_6_9&id=1bf477d3cdf1a864646d59820878783d42357a1d
URL	https://security.netapp.com/advisory/ntap-20181023-0001/

OpenSSL Deprecated Function 'RAND_pseudo_bytes' Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The openssl_random_pseudo_bytes function in ext/openssl/openssl.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 incorrectly relies on the deprecated RAND_pseudo_bytes function, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8867
URL	https://bugs.php.net/bug.php?id=70014
URL	http://git.php.net/?p=php-src.git;a=commit;h=16023f3e3b9c06cf677c3c980e8d574e4c162827

Type	Reference
URL	https://cwe.mitre.org/data/definitions/310.html
URL	http://www.php.net/ChangeLog-7.php
URL	https://bugs.launchpad.net/ubuntu/+source/php5/+bug/1534203

PHP 5.6.x and 7.x 'gdImageRotateInterpolated' Function Denial of Service — Medium

Vulnerability Details

The gdImageRotateInterpolated function in ext/gd/libgd/gd_interpolation.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a large bgd_color argument to the imagerotate function.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.4

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-1903
BUGTRAQ	http://www.securityfocus.com/bid/79916
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://www.php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=70976

PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 Remote Denial of Service Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

sapi/fpm/fpm/fpm_log.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 misinterprets the semantics of the snprintf return value, which allows attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read and buffer overflow) via a long string, as demonstrated by a long URI in a configuration with custom REQUEST_URI logging.

CVSS Base Score: 9.1

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5114
URL	https://bugs.php.net/bug.php?id=70755
URL	http://php.net/ChangeLog-7.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://www.search-lab.hu/about-us/news/111-some-unusual-vulnerabilities-in-the-php-engine
URL	http://github.com/php/php-src/commit/2721a0148649e07ed74468f097a28899741eb58f?w=1
URL	http://php.net/ChangeLog-5.php

PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3: Metadata can be set by an attacker

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

In PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3, all of the return values of stream_get_meta_data can be controlled if the input can be controlled (e.g., during file uploads). For example, a "$uri = stream_get_meta_data(fopen($file, "r"))['uri']" call mishandles the case where $file is data:text/plain;uri=eviluri, -- in other words, metadata can be set by an attacker.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10712
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://bugs.php.net/bug.php?id=71323
URL	https://git.php.net/?p=php-src.git;a=commit;h=6297a117d77fa3a0df2e21ca926a92c231819cd5

PHP 'before 5.6.32, 7.x before 7.0.25, 7.1.x before 7.1.11' Interpreter Information Leak Vulnerability

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In PHP before 5.6.32, 7.x before 7.0.25, and 7.1.x before 7.1.11, an error in the date extension's timelib_meridian handling of 'front of' and 'back of' directives could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: this is a different issue than CVE-2017-11145.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-16642
BUGTRAQ	http://www.securityfocus.com/bid/101745

Type	Reference
URL	https://github.com/derickr/timelib/commit/aa9156006e88565e1f1a5f7cc088b18322d57536
URL	https://github.com/php/php-src/commit/5c0455bf2c8cd3c25401407f158e820aa3b239e1
URL	https://cwe.mitre.org/data/definitions/125.html
URL	https://bugs.php.net/bug.php?id=75055
URL	http://php.net/ChangeLog-5.php
URL	http://php.net/ChangeLog-7.php
URL	https://security.netapp.com/advisory/ntap-20181123-0001/

PHP 'Bucket Brigade' Vulnerability — Medium

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

The Apache2 component in PHP before 5.6.38, 7.0.x before 7.0.32, 7.1.x before 7.1.22, and 7.2.x before 7.2.10 allows XSS via the body of a "Transfer-Encoding: chunked" request, because the bucket brigade is mishandled in the php_handler function in sapi/apache2handler/sapi_apache2.c.
Impact:
A cross-site scripting attack could be launched via the body of a "Transfer-Encoding: chunked" request.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-17082
URL	http://php.net/ChangeLog-5.php
URL	http://php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/79.html

Type	Reference
URL	https://security.netapp.com/advisory/ntap-20180924-0001/
URL	https://github.com/php/php-src/commit/23b057742e3cf199612fa8050ae86cae675e214e
URL	https://bugs.php.net/bug.php?id=76582
URL	http://php.net/downloads.php

PHP bz2.c 'bzread' Denial of Service — Medium

Vulnerability Details

The bzread function in ext/bz2/bz2.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted bz2 archive.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5399
BUGTRAQ	http://www.securityfocus.com/bid/92051
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1358395
URL	http://packetstormsecurity.com/files/137998/PHP-7.0.8-5.6.23-5.5.37-bzread-OOB-Write.html
URL	http://php.net/ChangeLog-5.php
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=72613

Type	Reference
URL	https://cwe.mitre.org/data/definitions/787.html

PHP 'cdf_check_stream_offset' Function Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The cdf_check_stream_offset function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, relies on incorrect sector-size data, which allows remote attackers to cause a denial of service (application crash) via a crafted stream offset in a CDF file.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3479
BUGTRAQ	http://www.securityfocus.com/bid/68241
URL	https://support.apple.com/HT204659
URL	http://support.apple.com/kb/HT6443
URL	https://github.com/file/file/commit/36fadd29849b8087af9f4586f89dbf74ea45be67
URL	https://bugs.php.net/bug.php?id=67411
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html

PHP cdf.c Integer Overflow Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Integer overflow in the cdf_read_property_info function in cdf.c in file through 5.19, as used in the Fileinfo component in PHP before 5.4.32 and 5.5.x before 5.5.16, allows remote attackers to cause a denial of service (application crash) via a crafted CDF file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1571.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3587
BUGTRAQ	http://www.securityfocus.com/bid/69325
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	http://php.net/ChangeLog-5.php
URL	https://github.com/file/file/commit/0641e56be1af003aa02c7c6b0184466540637233
URL	https://security-tracker.debian.org/tracker/CVE-2014-3587
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	https://bugs.php.net/bug.php?id=67716
URL	https://support.apple.com/HT204659
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
URL	https://github.com/php/php-src/commit/7ba1409a1aee5925180de546057ddd84ff267947

PHP 'cdf_count_chain' Function Denial of Service

Medium

Vulnerability Details

The cdf_count_chain function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate sector-count data, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3480
BUGTRAQ	http://www.securityfocus.com/bid/68238
URL	http://support.apple.com/kb/HT6443
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	https://bugs.php.net/bug.php?id=67412
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://github.com/file/file/commit/40bade80cbe2af1d0b2cd0420cebd5d5905a2382
URL	https://support.apple.com/HT204659

PHP 'cdf_read_property_info' Function Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The cdf_read_property_info function in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate a stream offset, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3487
BUGTRAQ	http://www.securityfocus.com/bid/68120
URL	https://support.apple.com/HT204659
URL	http://support.apple.com/kb/HT6443
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	https://github.com/file/file/commit/93e063ee374b6a75729df9e7201fb511e47e259d
URL	https://bugs.php.net/bug.php?id=67413
URL	https://cwe.mitre.org/data/definitions/20.html

PHP 'cdf_read_property_info' in Fileinfo Component Denial of Service

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The cdf_read_property_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0238
BUGTRAQ	http://www.securityfocus.com/bid/67765
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://github.com/file/file/commit/f97486ef5dc3e8735440edc4fc8808c63e1a3ef0
URL	https://bugs.php.net/bug.php?id=67327
URL	https://support.apple.com/HT204659
URL	http://support.apple.com/kb/HT6443
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html

PHP 'cdf_unpack_summary_info' in Fileinfo Component Denial of Service

Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0237
BUGTRAQ	http://www.securityfocus.com/bid/67759
URL	https://github.com/file/file/commit/b8acc83781d5a24cc5101e525d15efe0482c280d

Type	Reference
URL	https://bugs.php.net/bug.php?id=67328
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	https://support.apple.com/HT204659
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://support.apple.com/kb/HT6443

PHP 'data_len' Uninitialized Read Vulnerability — Medium

Vulnerability Details

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the data_len variable.
Impact:
An attacker could leverage this vulnerability to read the contents of memory to obtain information that could aid in launching further attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of PHP.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9639
URL	http://php.net/downloads.php
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://security.netapp.com/advisory/ntap-20190502-0007/

PHP dirstream.c 'phar_make_dirstream' Mishandled Zero-size Denial of Service — Medium

Vulnerability Details

The phar_make_dirstream function in ext/phar/dirstream.c in PHP before 5.6.18 and 7.x before 7.0.3 mishandles zero-size ././@LongLink files, which allows remote attackers to cause a denial of service (uninitialized pointer dereference) or possibly have unspecified other impact via a crafted TAR archive.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4343
BUGTRAQ	http://www.securityfocus.com/bid/89179
URL	http://php.net/ChangeLog-7.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://bugs.php.net/bug.php?id=71331
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	http://php.net/ChangeLog-5.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731

PHP dns.c 'php_parserr' Function Buffer Overflow Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Multiple buffer overflows in the php_parserr function in ext/standard/dns.c in PHP before 5.4.32 and 5.5.x before 5.5.16 allow remote DNS servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted DNS record, related to the dns_get_record function and the dn_expand function. NOTE: this issue exists because of an incomplete fix for CVE-2014-4049.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3597
BUGTRAQ	http://www.securityfocus.com/bid/69322
URL	https://bugs.php.net/bug.php?id=67717
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://php.net/ChangeLog-5.php
URL	https://support.apple.com/HT204659
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	https://github.com/php/php-src/commit/2fefae47716d501aec41c1102f3fd4531f070b05
URL	https://security-tracker.debian.org/tracker/CVE-2014-3597

PHP 'do_soap_call' Function Type Confusion Vulnerability — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The do_soap_call function in ext/soap/soap.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 does not verify that the uri property is a string, which allows remote attackers to obtain sensitive information by providing crafted serialized data with an int data type, related to a "type confusion" issue.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4148
BUGTRAQ	http://www.securityfocus.com/bid/75103
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://php.net/ChangeLog-5.php
URL	https://support.apple.com/kb/HT205031
URL	https://bugs.php.net/bug.php?id=69085

PHP exif.c 'exif_convert_any_to_int' Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exif_convert_any_to_int function in ext/exif/exif.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (application crash) via crafted EXIF data that triggers an attempt to divide the minimum representable negative integer by -1.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10158
BUGTRAQ	http://www.securityfocus.com/bid/95764
URL	http://php.net/ChangeLog-7.php
URL	https://www.tenable.com/security/tns-2017-04

Type	Reference
URL	https://github.com/php/php-src/commit/1cda0d7c2ffb62d8331c64e703131d9cabdc03ea
URL	https://bugs.php.net/bug.php?id=73737
URL	http://php.net/ChangeLog-5.php
URL	https://security.netapp.com/advisory/ntap-20180112-0001/

PHP exif.c 'exif_process_IFD_in_TIFF' Information Disclosure Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exif_process_IFD_in_TIFF function in ext/exif/exif.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7128
BUGTRAQ	http://www.securityfocus.com/bid/92564
URL	https://www.tenable.com/security/tns-2016-19
URL	https://bugs.php.net/bug.php?id=72627
URL	https://github.com/php/php-src/commit/6dbb1ee46b5f4725cc6519abf91e512a2a10dfed?w=1
URL	http://www.php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/200.html

PHP 'exif.c' Integer Overflow Vulnerability **Medium**

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.
Impact:
Successfully exploiting this issue may allow a remote attacker to crash the affected application, denying service to legitimate users. Due to the nature of this issue, code execution may be possible but this has not been confirmed.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-14883
BUGTRAQ	http://www.securityfocus.com/bid/104871
URL	https://www.tenable.com/security/tns-2018-12
URL	http://php.net/ChangeLog-7.php
URL	http://php.net/downloads.php
URL	https://security.netapp.com/advisory/ntap-20181107-0003/
URL	https://bugs.php.net/bug.php?id=76423
URL	https://cwe.mitre.org/data/definitions/190.html
URL	http://php.net/ChangeLog-5.php

PHP 'exif.c' Out-of-Bounds Read Vulnerability **Medium**

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.
Impact:
An attacker can exploit these issues to execute arbitrary code in the context of the affected application. Failed exploit attempts may result in a denial-of-service condition.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10549
BUGTRAQ	http://www.securityfocus.com/bid/104019
URL	http://php.net/downloads.php
URL	https://cwe.mitre.org/data/definitions/125.html
URL	http://php.net/ChangeLog-7.php
URL	https://www.synology.com/support/security/Synology_SA_18_20
URL	https://www.tenable.com/security/tns-2018-12
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=76130
URL	https://security.netapp.com/advisory/ntap-20180607-0003/

PHP 'EXIF' Extension Crafted JPEG Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3670
BUGTRAQ	http://www.securityfocus.com/bid/70665
URL	http://git.php.net/?p=php-src.git;a=commit;h=ddb207e7fa2e9adeba021a1303c3781efda5409b
URL	https://support.apple.com/HT204659
URL	http://linux.oracle.com/errata/ELSA-2014-1768.html
URL	http://linux.oracle.com/errata/ELSA-2014-1767.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1154502
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://bugs.php.net/bug.php?id=68113
URL	http://php.net/ChangeLog-5.php

PHP 'exif_process_SOFn' Invalid Read Vulnerability — Medium

Vulnerability Details

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an Invalid Read in exif_process_SOFn.
Impact:
An attacker could leverage this vulnerability to read the contents of memory to obtain information that could aid in launching further attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of PHP.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9640
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://security.netapp.com/advisory/ntap-20190502-0007/
URL	http://php.net/downloads.php

PHP 'exif_process_unicode' Function EXIF Data Denial of Service Flaw

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0232
BUGTRAQ	http://www.securityfocus.com/bid/72541
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://git.php.net/?p=php-src.git;a=commit;h=21bc7464f454fec18a9ec024c738f195602fee2a
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1185472
URL	http://git.php.net/?p=php-src.git;a=commit;h=2fc178cf448d8e1b95d1314e47eeef610729e0df

Type	Reference
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=68799
URL	http://advisories.mageia.org/MGASA-2015-0040.html
URL	https://support.apple.com/HT205267
URL	http://git.php.net/?p=php-src.git;a=commit;h=55001de6d8c6ed2aada870a76de1e4b4558737bf

PHP 'exif_process_user_comment' Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The exif_process_user_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6292
BUGTRAQ	http://www.securityfocus.com/bid/92078
URL	https://bugs.php.net/72618
URL	https://cwe.mitre.org/data/definitions/476.html
URL	http://php.net/ChangeLog-7.php
URL	https://support.apple.com/HT207170

Type	Reference
URL	http://git.php.net/?p=php-src.git;a=commit;h=41131cd41d2fd2e0c2f332a27988df75659c42e4
URL	http://php.net/ChangeLog-5.php

PHP 'ext/iconv/iconv.c' Infinite Loop Vulnerability — Medium

Vulnerability Details

An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.
Impact:
A remote user can cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10546
BUGTRAQ	http://www.securityfocus.com/bid/104019
URL	http://php.net/ChangeLog-7.php
URL	http://php.net/downloads.php
URL	https://security.netapp.com/advisory/ntap-20180607-0003/
URL	https://www.tenable.com/security/tns-2018-12
URL	https://bugs.php.net/bug.php?id=76249
URL	https://cwe.mitre.org/data/definitions/400.html
URL	http://php.net/ChangeLog-5.php

PHP 'ext/ldap/ldap.c' Denial of Service Vulnerability — Medium

Vulnerability Details

An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.
Impact:
A remote user can cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10548
BUGTRAQ	http://www.securityfocus.com/bid/104019
URL	https://www.tenable.com/security/tns-2018-12
URL	https://security.netapp.com/advisory/ntap-20180607-0003/
URL	http://php.net/ChangeLog-7.php
URL	http://php.net/downloads.php
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=76248
URL	https://cwe.mitre.org/data/definitions/476.html

PHP 'ext/phar/phar.c' Buffer Over-read Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read and application crash) via a crafted length value in conjunction with crafted serialized data in a phar archive, related to the phar_parse_metadata and phar_parse_pharfile functions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2783
BUGTRAQ	http://www.securityfocus.com/bid/74239
URL	https://support.apple.com/kb/HT205031
URL	https://support.apple.com/HT205267
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	https://bugs.php.net/bug.php?id=69324
URL	http://php.net/ChangeLog-5.php

PHP 'ext/phar/phar_object.c' Cross-site Scripting Vulnerability Medium

Vulnerability Details

An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.
Impact:
An attacker may leverage this vulnerability to execute arbitrary HTML and JavaScript in the browser of an unsuspecting user in the context of the affected site. This may let the attacker steal cookie-based authentication credentials and launch other attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10547
URL	https://www.tenable.com/security/tns-2018-12
URL	http://php.net/downloads.php
URL	http://php.net/ChangeLog-7.php
URL	https://security.netapp.com/advisory/ntap-20180607-0003/
URL	https://bugs.php.net/bug.php?id=76129
URL	https://cwe.mitre.org/data/definitions/79.html
URL	http://php.net/ChangeLog-5.php

PHP 'ext/spl/spl_array.c' Denial of Service Vulnerability — Medium

Vulnerability Details

Use-after-free vulnerability in ext/spl/spl_array.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted ArrayIterator usage within applications in certain web-hosting environments.
Impact:
An attacker could cause a denial of service condition on the asset.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.6

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4698
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	http://php.net/downloads.php
URL	https://bugs.php.net/bug.php?id=67539
URL	https://support.apple.com/HT204659

PHP 'ext/spl/spl_dllist.c' Denial of Service Vulnerability

Medium

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

Use-after-free vulnerability in ext/spl/spl_dllist.c in the SPL component in PHP through 5.5.14 allows context-dependent attackers to cause a denial of service or possibly have unspecified other impact via crafted iterator usage within applications in certain web-hosting environments.
Impact:
An attacker could cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.6

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4670
URL	http://php.net/downloads.php
URL	https://support.apple.com/HT204659
URL	https://bugs.php.net/bug.php?id=67538
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html

PHP Fileinfo Component Denial of Service

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted CDF file.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0207
BUGTRAQ	http://www.securityfocus.com/bid/68243
URL	https://github.com/file/file/commit/6d209c1c489457397a5763bca4b28e43aac90391
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	http://support.apple.com/kb/HT6443
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1091842
URL	https://support.apple.com/HT204659
URL	https://bugs.php.net/bug.php?id=67326

PHP 'Fileinfo' Component Denial of Service Vulnerability

Medium

Vulnerability Details

file before 5.18, as used in the Fileinfo component in PHP before 5.6.0, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a zero root_storage value in a CDF file, related to cdf.c and readcdf.c.

Impact:
An attacker could cause a denial of service condition on the target asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0236
URL	http://git.php.net/?p=php-src.git;a=commit;h=f3f22ff5c697aef854ffc1918bce708b37481b0f
URL	http://php.net/downloads.php
URL	https://bugs.php.net/bug.php?id=67329
URL	http://php.net/ChangeLog-5.php

PHP Fileinfo Component Pascal String Denial of Service Flaw — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The mconvert function in softmagic.c in file before 5.21, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not properly handle a certain string-length field during a copy of a truncated version of a Pascal string, which might allow remote attackers to cause a denial of service (out-of-bounds memory access and application crash) via a crafted file.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9652
BUGTRAQ	http://www.securityfocus.com/bid/72505
URL	https://support.apple.com/HT205267
URL	http://bugs.gw.com/view.php?id=398
URL	https://bugs.php.net/bug.php?id=68735
URL	https://bugs.php.net/patch-display.php?bug=68735&patch=bug68735.patch&revision=1420309079
URL	https://github.com/file/file/commit/59e63838913eee47f5c120a6c53d4565af638158
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://cwe.mitre.org/data/definitions/119.html

PHP 'fsockopen' Server-Side Request Forgery Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

PHP through 7.1.11 enables potential SSRF in applications that accept an fsockopen or pfsockopen hostname argument with an expectation that the port number is constrained. Because a :port syntax is recognized, fsockopen will use the port number that is specified in the hostname argument, instead of the port number in the second argument of the function.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.4

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7272
BUGTRAQ	http://www.securityfocus.com/bid/97178
URL	https://github.com/php/php-src/commit/bab0b99f376dac9170ac81382a5ed526938d595a
URL	https://bugs.php.net/bug.php?id=75505
URL	https://cwe.mitre.org/data/definitions/918.html
URL	https://www.sec-consult.com/fxdata/seccons/prod/temedia/advisories_txt/20170403-0_PHP_Misbehavior_of_fsockopen_function_v10.txt
URL	https://bugs.php.net/bug.php?id=74216
URL	https://security.netapp.com/advisory/ntap-20180112-0001/

PHP '_gd2GetHeader' Denial of Service Vulnerability — Medium

Vulnerability Details

Integer overflow in the _gd2GetHeader function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via crafted chunk dimensions in an image.
Impact:
A remote attacker could possibly execute arbitrary code within the context of the process or cause a denial of service condition.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5766

Type	Reference
URL	https://bugs.php.net/bug.php?id=72339
URL	http://github.com/php/php-src/commit/7722455726bec8c53458a32851d2a87982cf0eac?w=1
URL	https://cwe.mitre.org/data/definitions/190.html
URL	http://php.net/downloads.php
URL	http://php.net/ChangeLog-7.php
URL	https://libgd.github.io/release-2.2.3.html
URL	http://php.net/ChangeLog-5.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731

PHP 'gd.c' Denial of Service Vulnerability

Medium

Vulnerability Details

Stack consumption vulnerability in the gdImageFillToBorder function in gd.c in the GD Graphics Library (aka libgd) before 2.2.2, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (segmentation violation) via a crafted imagefilltoborder call that triggers use of a negative color value.
Impact:
An attacker could cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9933
BUGTRAQ	http://www.securityfocus.com/bid/94865

Type	Reference
URL	http://www.php.net/ChangeLog-7.php
URL	https://github.com/php/php-src/commit/863d37ea66d5c960db08d6f4a2cbd2518f0f80d1
URL	https://github.com/libgd/libgd/issues/215
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://github.com/libgd/libgd/commit/77f619d48259383628c3ec4654b1ad578e9eb40e
URL	https://bugs.php.net/bug.php?id=72696
URL	http://php.net/downloads.php

PHP 'gd_crop.c' Denial of Service Vulnerability — Medium

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

The gdImageCropThreshold function in gd_crop.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 7.0.9, allows remote attackers to cause a denial of service (application crash) via an invalid color index.
Impact:
An attacker could cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6128
BUGTRAQ	http://www.securityfocus.com/bid/91509
URL	https://bugs.php.net/72494

Type	Reference
URL	https://github.com/libgd/libgd/commit/1ccfe21e14c4d18336f9da8515cd17db88c3de61
URL	https://libgd.github.io/release-2.2.3.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://php.net/downloads.php
URL	https://github.com/libgd/libgd/commit/6ff72ae40c7c20ece939afb362d98cc37f4a1c96

PHP gd_ctx.c Arbitrary File Overwrite Vulnerabilty — Medium

Vulnerability Details

gd_ctx.c in the GD component in PHP 5.4.x before 5.4.32 and 5.5.x before 5.5.16 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to overwrite arbitrary files via crafted input to an application that calls the (1) imagegd, (2) imagegd2, (3) imagegif, (4) imagejpeg, (5) imagepng, (6) imagewbmp, or (7) imagewebp function.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 6.4

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-5120
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=67730
URL	https://support.apple.com/HT204659

PHP gd_gif_in.c Crafted GIF Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1, has an integer signedness error that leads to an infinite loop via a crafted GIF file, as demonstrated by a call to the imagecreatefromgif or imagecreatefromstring PHP function. This is related to GetCode_ and gdImageCreateFromGifCtx.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5711
URL	https://cwe.mitre.org/data/definitions/400.html
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=75571
URL	http://php.net/ChangeLog-7.php

PHP gd_gif_in.c 'gdImageCreateFromGifCtx' Information Disclosure — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read ~700 bytes from the top of the stack, potentially disclosing sensitive information.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7890
BUGTRAQ	http://www.securityfocus.com/bid/99492
URL	https://bugs.php.net/bug.php?id=74435
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://php.net/ChangeLog-5.php
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	https://bugs.php.net/patch-display.php?bug=74435&patch=fix-74435-php-7.0&revision=1497970038
URL	http://php.net/ChangeLog-7.php
URL	https://www.tenable.com/security/tns-2017-12

PHP 'gdImageCreate' Denial of Service Vulnerability — Medium

Vulnerability Details

Integer overflow in the gdImageCreate function in gd.c in the GD Graphics Library (aka libgd) before 2.0.34RC1, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted image dimensions.
Impact:
An attacker could cause a denial of service condition on the asset.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5767
BUGTRAQ	http://www.securityfocus.com/bid/91395
URL	http://php.net/downloads.php
URL	https://bugs.php.net/bug.php?id=72446
URL	http://github.com/php/php-src/commit/c395c6e5d7e8df37a21265ff76e48fe75ceb5ae6?w=1
URL	http://php.net/ChangeLog-5.php
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/190.html

PHP 'gd_interpolation.c' Denial of Service Vulnerability — Medium

Vulnerability Details

gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.1.1, as used in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7, allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted image that is mishandled by the imagescale function.
Impact:
An attacker could cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-7456

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/90859
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	https://github.com/php/php-src/commit/7a1aac3343af85b4af4df5f8844946eaa27394ab?w=1
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=72227
URL	https://cwe.mitre.org/data/definitions/125.html
URL	http://php.net/downloads.php
URL	https://github.com/libgd/libgd/commit/4f65a3e4eedaffa1efcf9ee1eb08f0b504fbc31a
URL	http://php.net/ChangeLog-5.php

PHP gd_interpolation.c 'gdImageScaleTwoPass' Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The gdImageScaleTwoPass function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in PHP before 5.6.12, uses inconsistent allocate and free approaches, which allows remote attackers to cause a denial of service (memory consumption) via a crafted call, as demonstrated by a call to the PHP imagescale function.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8877

Type	Reference
URL	https://github.com/libgd/libgd/commit/4751b606fa38edc456d627140898a7ec679fcc24
URL	https://github.com/libgd/libgd/issues/173
URL	https://cwe.mitre.org/data/definitions/399.html
URL	https://bugs.php.net/bug.php?id=70064

PHP 'GetCode_' Function Crafted GIF Image Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The GetCode_ function in gd_gif_in.c in GD 2.1.1 and earlier, as used in PHP before 5.5.21 and 5.6.x before 5.6.5, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted GIF image that is improperly handled by the gdImageCreateFromGif function.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9709
BUGTRAQ	http://www.securityfocus.com/bid/73306
URL	http://advisories.mageia.org/MGASA-2015-0040.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinapr2015-2511959.html
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=68601

Type	Reference
URL	https://bitbucket.org/libgd/gd-libgd/commits/47eb44b2e90ca88a08dca9f9a1aa9041e9587f43
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://support.apple.com/HT205267
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1188639

PHP GMP Interfaces Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

** DISPUTED ** The GNU Multiple Precision Arithmetic Library (GMP) interfaces for PHP through 7.1.4 allow attackers to cause a denial of service (memory consumption and application crash) via operations on long strings. NOTE: the vendor disputes this, stating "There is no security issue here, because GMP safely aborts in case of an OOM condition. The only attack vector here is denial of service. However, if you allow attacker-controlled, unbounded allocations you have a DoS vector regardless of GMP's OOM behavior."

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-7963
URL	https://cwe.mitre.org/data/definitions/399.html
URL	https://bugs.php.net/bug.php?id=74308

PHP HTTP_PROXY Environment Variable Namespace Conflict — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, as demonstrated by (1) an application that makes a getenv('HTTP_PROXY') call or (2) a CGI configuration of PHP, aka an "httpoxy" issue.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.1

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-5385
BUGTRAQ	http://www.securityfocus.com/bid/91821
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1353794
URL	https://cwe.mitre.org/data/definitions/284.html
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
URL	https://httpoxy.org/
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05333297
URL	https://www.drupal.org/SA-CORE-2016-003
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03770en_us

Type	Reference
URL	https://github.com/guzzle/guzzle/releases/tag/6.2.1
URL	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html

PHP 'imagefilltoborder' Denial of Service — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Stack consumption vulnerability in GD in PHP before 5.6.12 allows remote attackers to cause a denial of service via a crafted imagefilltoborder call.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8874
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://bugs.php.net/bug.php?id=66387
URL	http://php.net/ChangeLog-5.php

PHP JPEG Denial of Service Vulnerability — Medium

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before

7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.
Impact:
An attacker could cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-14851
BUGTRAQ	http://www.securityfocus.com/bid/104871
URL	http://php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/125.html
URL	https://security.netapp.com/advisory/ntap-20181107-0003/
URL	http://php.net/downloads.php
URL	http://php.net/ChangeLog-5.php
URL	https://www.tenable.com/security/tns-2018-12
URL	https://bugs.php.net/bug.php?id=76557

PHP 'linkinfo' File Path Disclosure Vulnerability — Medium

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

An issue was discovered in ext/standard/link_win32.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. The linkinfo function on Windows doesn't implement the open_basedir check. This could be abused to find files on paths outside of the allowed directories.
Impact:
An attacker could obtain file paths they should not have permissions to see.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-15132
URL	https://github.com/php/php-src/commit/f151e048ed27f6f4eef729f3310d053ab5da71d4
URL	http://php.net/downloads.php
URL	https://bugs.php.net/bug.php?id=76459
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://php.net/ChangeLog-7.php
URL	https://security.netapp.com/advisory/ntap-20181107-0003/
URL	http://php.net/ChangeLog-5.php
URL	https://www.tenable.com/security/tns-2018-12

PHP "main/php_open_temporary_file.c" Thread Safety Denial of Service Flaw

Medium

Vulnerability Details

main/php_open_temporary_file.c in PHP before 5.5.28 and 5.6.x before 5.6.12 does not ensure thread safety, which allows remote attackers to cause a denial of service (race condition and heap memory corruption) by leveraging an application that performs many temporary-file accesses.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 5.9

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8878
URL	https://bugs.php.net/bug.php?id=70002

PHP 'make_http_soap_request' Function Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The make_http_soap_request function in ext/soap/php_http.c in PHP before 5.4.44, 5.5.x before 5.5.28, 5.6.x before 5.6.12, and 7.x before 7.0.4 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (type confusion and application crash) via crafted serialized _cookies data, related to the SoapClient::__call method in ext/soap/soap.c.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.1

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-3185
BUGTRAQ	http://www.securityfocus.com/bid/84307
URL	https://git.php.net/?p=php-src.git;a=commit;h=eaf4e77190d402ea014207e9a7d5da1a4f3727ba
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=71610
URL	https://bugs.php.net/bug.php?id=70081

PHP 'mconvert' Function Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Buffer overflow in the mconvert function in softmagic.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (application crash) via a crafted Pascal string in a FILE_PSTRING conversion.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3478
BUGTRAQ	http://www.securityfocus.com/bid/68239
URL	https://support.apple.com/HT204659
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	http://support.apple.com/kb/HT6443
URL	https://github.com/file/file/commit/27a14bc7ba285a0a5ebfdb55e54001aa11932b08
URL	https://bugs.php.net/bug.php?id=67410
URL	https://cwe.mitre.org/data/definitions/119.html

PHP 'mcopy' Function Fileinfo Component Denial of Service — Medium

Vulnerability Details

The mcopy function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly restrict a certain offset value, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4605
BUGTRAQ	http://www.securityfocus.com/bid/75233
URL	https://bugs.php.net/bug.php?id=68819
URL	http://git.php.net/?p=php-src.git;a=commit;h=f938112c495b0d26572435c0be73ac0bfe642ecd
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://php.net/ChangeLog-5.php

PHP 'mget' Function Fileinfo Component Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The mget function in softmagic.c in file 5.x, as used in the Fileinfo component in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, does not properly maintain a certain pointer relationship, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted string that is mishandled by a "Python script text executable" rule.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4604

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/75241
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=68819
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://php.net/ChangeLog-5.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=f938112c495b0d26572435c0be73ac0bfe642ecd

PHP 'mod_php' Or 'php-fpm' Information Disclosure

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

An issue was discovered in PHP 5.x and 7.x, when the configuration uses apache2handler/mod_php or php-fpm with OpCache enabled. With 5.x after 5.6.28 or 7.x after 7.0.13, the issue is resolved in a non-default configuration with the opcache.validate_permission=1 setting. The vulnerability details are as follows. In PHP SAPIs where PHP interpreters share a common parent process, Zend OpCache creates a shared memory object owned by the common parent during initialization. Child PHP processes inherit the SHM descriptor, using it to cache and retrieve compiled script bytecode ("opcode" in PHP jargon). Cache keys vary depending on configuration, but filename is a central key component, and compiled opcode can generally be run if a script's filename is known or can be guessed. Many common shared-hosting configurations change EUID in child processes to enforce privilege separation among hosted users (for example using mod_ruid2 for the Apache HTTP Server, or php-fpm user settings). In these scenarios, the default Zend OpCache behavior defeats script file permissions by sharing a single SHM cache among all child PHP processes. PHP scripts often contain sensitive information: Think of CMS configurations where reading or running another user's script usually means gaining privileges to the CMS database.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8994
URL	http://marc.info/?l=php-internals&m=147921016724565&w=2
URL	http://marc.info/?l=php-internals&m=147876797317925&w=2
URL	https://ma.ttias.be/a-better-way-to-run-php-fpm/
URL	https://bugs.php.net/bug.php?id=69090
URL	http://seclists.org/oss-sec/2017/q1/520
URL	http://seclists.org/oss-sec/2016/q4/343
URL	http://openwall.com/lists/oss-security/2017/02/28/1

PHP 'move_uploaded_file' Extension Restrictions Bypass Flaw — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The move_uploaded_file implementation in ext/standard/basic_functions.c in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 truncates a pathname upon encountering a \x00 character, which allows remote attackers to bypass intended extension restrictions and create files with unexpected names via a crafted second argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2348
BUGTRAQ	http://www.securityfocus.com/bid/73434
URL	https://support.apple.com/HT205267

Type	Reference
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=69207
URL	http://git.php.net/?p=php-src.git;a=commit;h=1291d6bbee93b6109eb07e8f7916ff1b7fcc13e1
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://php.net/ChangeLog-5.php

PHP msgformat_format.c 'MessageFormatter::formatMessage' Denial of Service Vulnerability

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/intl/msgformat/msgformat_format.c in PHP before 5.6.26 and 7.x before 7.0.11 does not properly restrict the locale length provided to the Locale class in the ICU library, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a MessageFormatter::formatMessage call with a long first argument.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7416
BUGTRAQ	http://www.securityfocus.com/bid/93008
URL	http://www.php.net/ChangeLog-7.php
URL	https://www.tenable.com/security/tns-2016-19
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference
URL	https://bugs.php.net/bug.php?id=73007
URL	https://github.com/php/php-src/commit/6d55ba265637d6adf0ba7e9c9ef11187d1ec2f5b?w=1

PHP 'multipart_buffer_headers' Function Algorithmic Complexity Vulnerability

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/rfc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4024
BUGTRAQ	http://www.securityfocus.com/bid/74903
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05045763
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	https://support.apple.com/kb/HT205031
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://php.net/ChangeLog-5.php

Type	Reference
URL	https://bugs.php.net/bug.php?id=69364

PHP Multiple Pathname Sanitization Remote Arbitrary File Access Vulnerabilities — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read or write to arbitrary files via crafted input to an application that calls (1) a DOMDocument load method, (2) the xmlwriter_open_uri function, (3) the finfo_file function, or (4) the hash_hmac_file function, as demonstrated by a filename\0.xml attack that bypasses an intended configuration in which client users may read only .xml files.

CVSS Base Score: 6.4

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3411
BUGTRAQ	http://www.securityfocus.com/bid/75255
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	http://git.php.net/?p=php-src.git;a=commit;h=4435b9142ff9813845d5c97ab29a5d637bedb257
URL	https://bugs.php.net/bug.php?id=69353

PHP mysqlnd Man in the Middle via Cleartext-downgrade — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/mysqlnd/mysqlnd.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 uses a client SSL option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, a related issue to CVE-2015-3152.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.9

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8838
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=69669
URL	http://git.php.net/?p=php-src.git;a=commit;h=97aa752fee61fccdec361279adbfb17a3c60f3f4
URL	https://cwe.mitre.org/data/definitions/284.html

PHP mysqlnd_wireprotocol.c BIT Field Heap Buffer Overflow — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/mysqlnd/mysqlnd_wireprotocol.c in PHP before 5.6.26 and 7.x before 7.0.11 does not verify that a BIT field has the UNSIGNED_FLAG flag, which allows remote MySQL servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted field metadata.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7412
BUGTRAQ	http://www.securityfocus.com/bid/93005
URL	https://www.tenable.com/security/tns-2016-19
URL	https://github.com/php/php-src/commit/28f80baf3c53e267c9ce46a2a0fadbb981585132?w=1
URL	https://bugs.php.net/bug.php?id=72293
URL	http://www.php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/119.html

PHP Non-Blocking STDIN Stream Denial of Service Vulnerability — Medium

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.
Impact:
An attacker could cause a denial of service condition on the asset.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:L/Au:S/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-9253
URL	http://php.net/downloads.php
URL	https://www.futureweb.at/Futureweb-OG-php-fpm-master-process-restarts-child-process-in-a_pid,54177,type,firmeninfo.html

Type	Reference
URL	https://www.futureweb.at/security/CVE-2015-9253/
URL	https://bugs.php.net/bug.php?id=75968
URL	https://bugs.php.net/bug.php?id=70185
URL	https://bugs.php.net/bug.php?id=73342https://github.com/php/php-src/pull/3287
URL	https://cwe.mitre.org/data/definitions/400.html
URL	https://github.com/php/php-src/commit/69dee5c732fe982c82edb17d0dbc3e79a47748d8
URL	https://github.com/php/php-src/blob/PHP-7.1.20/NEWS#L20-L22

PHP "odbc_bindcols" Function Denial of Service Flaw — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The odbc_bindcols function in ext/odbc/php_odbc.c in PHP before 5.6.12 mishandles driver behavior for SQL_WVARCHAR columns, which allows remote attackers to cause a denial of service (application crash) in opportunistic circumstances by leveraging use of the odbc_fetch_array function to access a certain type of Microsoft SQL Server table.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8879
URL	https://bugs.php.net/bug.php?id=69975
URL	https://cwe.mitre.org/data/definitions/20.html

PHP openssl.c Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, the openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function, which could lead to a crash of the PHP interpreter, related to an interpretation conflict for a negative number in ext/openssl/openssl.c, and an OpenSSL documentation omission.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11144
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	https://bugs.php.net/bug.php?id=74651
URL	http://php.net/ChangeLog-5.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=91826a311dd37f4c4e5d605fa7af331e80ddd4c3
URL	https://www.tenable.com/security/tns-2017-12
URL	http://git.php.net/?p=php-src.git;a=commit;h=89637c6b41b510c20d262c17483f582f115c66d6
URL	http://git.php.net/?p=php-src.git;a=commit;h=73cabfedf519298e1a11192699f44d53c529315e
URL	http://php.net/ChangeLog-7.php
URL	http://openwall.com/lists/oss-security/2017/07/10/6
URL	https://cwe.mitre.org/data/definitions/754.html

PHP parse_date.c 'php_parse_date' Information Disclosure — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, an error in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: the correct fix is in the e8b7698f5ee757ce2c8bd10a192a491a498f891c commit, not the bd77ac90d3bdf31ce2a5251ad92e9e75 gist.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11145
BUGTRAQ	http://www.securityfocus.com/bid/99550
URL	https://www.tenable.com/security/tns-2017-12
URL	http://openwall.com/lists/oss-security/2017/07/10/6
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://php.net/ChangeLog-7.php
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	https://bugs.php.net/bug.php?id=74819
URL	https://gist.github.com/anonymous/bd77ac90d3bdf31ce2a5251ad92e9e75
URL	http://git.php.net/?p=php-src.git;a=commit;h=e8b7698f5ee757ce2c8bd10a192a491a498f891c
URL	http://php.net/ChangeLog-5.php

PHP PHAR 404 Error Page Reflected Cross-Site Scripting — Medium

Vulnerability Details

An issue was discovered in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1. There is Reflected XSS on the PHAR 404 error page via the URI of a request for a .phar file.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-5712
BUGTRAQ	http://www.securityfocus.com/bid/102742
BUGTRAQ	http://www.securityfocus.com/bid/104020
URL	http://php.net/ChangeLog-7.php
URL	https://bugs.php.net/bug.php?id=74782
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/79.html

PHP phar.c 'phar_parse_pharfile' Denial of Service — Medium

Vulnerability Details

Integer overflow in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory consumption or application crash) via a truncated manifest entry in a PHAR archive.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10159
BUGTRAQ	http://www.securityfocus.com/bid/95774
URL	http://php.net/ChangeLog-5.php
URL	http://php.net/ChangeLog-7.php
URL	https://www.tenable.com/security/tns-2017-04
URL	https://bugs.php.net/bug.php?id=73764
URL	https://github.com/php/php-src/commit/ca46d0acbce55019b970fcd4c1e8a10edfdded93
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	https://cwe.mitre.org/data/definitions/190.html

PHP phar.c 'phar_parse_pharfile' Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In PHP before 5.6.30 and 7.x before 7.0.15, the PHAR archive handler could be used by attackers supplying malicious archive files to crash the PHP interpreter or potentially disclose information due to a buffer over-read in the phar_parse_pharfile function in ext/phar/phar.c.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.1

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11147
BUGTRAQ	http://www.securityfocus.com/bid/99607
URL	http://php.net/ChangeLog-5.php

Type	Reference
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	http://php.net/ChangeLog-7.php
URL	http://openwall.com/lists/oss-security/2017/07/10/6
URL	https://www.tenable.com/security/tns-2017-12
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://bugs.php.net/bug.php?id=73773
URL	http://git.php.net/?p=php-src.git;a=commit;h=e5246580a85f031e1a3b8064edbaa55c1643a451

PHP PharData 'extractTo' Directory Traversal — Medium

Vulnerability Details

Directory traversal vulnerability in the PharData class in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to write to arbitrary files via a .. (dot dot) in a ZIP archive entry that is mishandled during an extractTo call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6833
URL	https://bugs.php.net/bug.php?id=70019
URL	https://cwe.mitre.org/data/definitions/22.html

PHP 'phar_parse_tarfile' Function Denial of Service — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not verify that the first character of a filename is different from the \0 character, which allows remote attackers to cause a denial of service (integer underflow and memory corruption) via a crafted entry in a tar archive.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4021
BUGTRAQ	http://www.securityfocus.com/bid/74700
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://support.apple.com/kb/HT205031
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=69453

PHP 'php_handler' Function Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The php_handler function in sapi/apache2handler/sapi_apache2.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8, when the Apache HTTP Server 2.4.x is used, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via pipelined HTTP requests that result in a "deconfigured interpreter."

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3330
BUGTRAQ	http://www.securityfocus.com/bid/74204
URL	https://support.apple.com/HT205267
URL	https://bugs.php.net/bug.php?id=69218
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://php.net/ChangeLog-5.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=809610f5ea38a83b284e1125d1fff129bdd615e7
URL	https://support.apple.com/kb/HT205031
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=68486

PHP 'php_imap.c' Denial of Service Vulnerability — Medium

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of PHP.

Vulnerability Details

ext/imap/php_imap.c in PHP 5.x and 7.x before 7.3.0 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty string in the message argument to the imap_mail function.
Impact:
Attackers can exploit this issue to cause denial-of-service condition, denying service to legitimate users.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-19935
BUGTRAQ	http://www.securityfocus.com/bid/106143
URL	http://php.net/downloads.php
URL	https://cwe.mitre.org/data/definitions/476.html
URL	https://security.netapp.com/advisory/ntap-20181221-0003/
URL	https://bugs.php.net/bug.php?id=77020

PHP 'php_raw_url_encode' Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

** DISPUTED ** Integer overflow in the php_raw_url_encode function in ext/standard/url.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to cause a denial of service (application crash) via a long string to the rawurlencode function. NOTE: the vendor says "Not sure if this qualifies as security issue (probably not)."

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-4070
BUGTRAQ	http://www.securityfocus.com/bid/85801
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://support.apple.com/HT206567
URL	https://git.php.net/?p=php-src.git;a=commit;h=95433e8e339dbb6b5d5541473c1661db6ba2c451

Type	Reference
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://bugs.php.net/bug.php?id=71798
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05240731
URL	http://www.php.net/ChangeLog-7.php

PHP 'php_stream_zip_opener' Stack Buffer Overflow — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6297
BUGTRAQ	http://www.securityfocus.com/bid/92099
URL	http://git.php.net/?p=php-src.git;a=commit;h=81406c0c1d45f75fcc7972ed974d2597abb0b9e9
URL	https://bugs.php.net/72520
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/119.html
URL	http://fortiguard.com/advisory/fortinet-discovers-php-stack-based-buffer-overflow-vulnerabilities

Type	Reference
URL	http://php.net/ChangeLog-7.php
URL	https://support.apple.com/HT207170

PHP php_variables.c Denial of Service — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In PHP before 5.6.31, 7.x before 7.0.17, and 7.1.x before 7.1.3, remote attackers could cause a CPU consumption denial of service attack by injecting long form variables, related to main/php_variables.c.

CVSS Base Score: 7.8

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11142
BUGTRAQ	http://www.securityfocus.com/bid/99601
URL	http://php.net/ChangeLog-7.php
URL	http://openwall.com/lists/oss-security/2017/07/10/6
URL	https://cwe.mitre.org/data/definitions/400.html
URL	https://bugs.php.net/bug.php?id=73807
URL	https://github.com/php/php-src/commit/a15bffd105ac28fd0dd9b596632dbf035238fda3
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	http://php.net/ChangeLog-5.php
URL	https://www.tenable.com/security/tns-2017-12

Type	Reference
URL	https://github.com/php/php-src/commit/0f8cf3b8497dc45c010c44ed9e96518e11e19fc3

PHP PostgreSQL 'build_tablename' Function Denial of Service Flaw — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The build_tablename function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP through 5.6.7 does not validate token extraction for table names, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-1352
BUGTRAQ	http://www.securityfocus.com/bid/71932
URL	https://bugs.php.net/bug.php?id=68741
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://git.php.net/?p=php-src.git;a=commit;h=124fb22a13fafa3648e4e15b4f207c7096d8155e
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://support.apple.com/HT205267

PHP PostgreSQL Extension 'php_pgsql_meta_data' Function Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The php_pgsql_meta_data function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not validate token extraction for table names, which might allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1352.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4644
BUGTRAQ	http://www.securityfocus.com/bid/75292
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html
URL	https://bugs.php.net/bug.php?id=69667
URL	http://php.net/ChangeLog-5.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=2cc4e69cc6d8dbc4b3568ad3dd583324a7c11d64

PHP 'rename()' Sensitive Data Disclosure Vulnerability — Medium

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of PHP.

Vulnerability Details

An issue was discovered in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. Due to the way rename() across filesystems is implemented, it is possible that file being renamed is briefly available with wrong permissions while the rename is ongoing, thus enabling unauthorized users to access the data.
Impact:
An attacker could leverage this vulnerability to gain access to file data without authorization.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9637
URL	https://support.f5.com/csp/article/K53825211
URL	http://php.net/downloads.php
URL	https://security.netapp.com/advisory/ntap-20190502-0007/

PHP 'sapi_header_op' Function Cross-Site Scripting Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The sapi_header_op function in main/SAPI.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 supports deprecated line folding without considering browser compatibility, which allows remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer by leveraging (1) %0A%20 or (2) %0D%0A%20 mishandling in the header function.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.1

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8935
URL	https://github.com/php/php-src/commit/996faf964bba1aec06b153b370a7f20d3dd2bb8b?w=1
URL	https://bugs.php.net/bug.php?id=68978
URL	https://cwe.mitre.org/data/definitions/79.html

PHP session.c Invalid Session Names Object Injection — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

ext/session/session.c in PHP before 5.6.25 and 7.x before 7.0.10 skips invalid session names in a way that triggers incorrect parsing, which allows remote attackers to inject arbitrary-type session data by leveraging control of a session name, as demonstrated by object injection.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7125
BUGTRAQ	http://www.securityfocus.com/bid/92552
URL	https://www.tenable.com/security/tns-2016-19
URL	https://bugs.php.net/bug.php?id=72681
URL	https://github.com/php/php-src/commit/8763c6090d627d8bb0ee1d030c30e58f406be9ce?w=1
URL	http://www.php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/74.html

PHP 'stream_resolve_include_path ' Function Pathname Sanitization Remote Arbitrary File Access Vulnerability — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to read arbitrary files via crafted input to an application that calls the stream_resolve_include_path function in ext/standard/streamsfuncs.c, as demonstrated by a filename\0.extension attack that bypasses an intended configuration in which client users may read files with only one specific extension.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-3412
BUGTRAQ	http://www.securityfocus.com/bid/75250
URL	https://bugs.php.net/bug.php?id=69353
URL	http://git.php.net/?p=php-src.git;a=commit;h=4435b9142ff9813845d5c97ab29a5d637bedb257
URL	http://php.net/ChangeLog-5.php
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjan2016-2867209.html

PHP url.c 'parse_url' Restriction Bypass — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In PHP before 5.6.28 and 7.x before 7.0.13, incorrect handling of various URI components in the URL parser could be used by attackers to bypass hostname-specific URL checks, as demonstrated by evil.example.com:80#@good.example.com/ and evil.example.com:80?@good.example.com/ inputs to the parse_url function (implemented in the php_url_parse_ex function in ext/standard/url.c).

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10397

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/99552
URL	http://openwall.com/lists/oss-security/2017/07/10/6
URL	http://git.php.net/?p=php-src.git;a=commit;h=b061fa909de77085d3822a89ab901b934d0362c4
URL	https://bugs.php.net/bug.php?id=73192
URL	http://php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	http://php.net/ChangeLog-5.php

PHP util.c 'phar_get_entry_data' Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The phar_get_entry_data function in ext/phar/util.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a .phar file with a crafted TAR archive entry in which the Link indicator references a file that does not exist.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7803
BUGTRAQ	http://www.securityfocus.com/bid/76959
URL	https://bugs.php.net/bug.php?id=69720

Type	Reference
URL	http://git.php.net/?p=php-src.git;a=commit;h=d698f0ae51f67c9cce870b09c59df3d6ba959244
URL	https://support.apple.com/HT205637

PHP 'value_len' Uninitialized Read Vulnerability — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of PHP.

Vulnerability Details

An issue was discovered in the EXIF component in PHP before 7.1.27, 7.2.x before 7.2.16, and 7.3.x before 7.3.3. There is an uninitialized read in exif_process_IFD_in_MAKERNOTE because of mishandling the maker_note->offset relationship to value_len.
Impact:
An attacker could leverage this vulnerability to read the contents of memory to obtain information that could aid in launching further attacks.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9638
URL	https://security.netapp.com/advisory/ntap-20190502-0007/
URL	http://php.net/downloads.php
URL	https://cwe.mitre.org/data/definitions/119.html

PHP 'var_unserializer.c' Denial of Service Vulnerability — Medium

Vulnerability Details

ext/standard/var_unserializer.c in PHP 5.x through 7.1.24 allows attackers to cause a denial of service (application crash) via an unserialize call for the com, dotnet, or variant class.
Impact:
Attackers can exploit these issues to crash the affected application, denying service to legitimate users.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of PHP.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-19396
BUGTRAQ	http://www.securityfocus.com/bid/105989
URL	https://security.netapp.com/advisory/ntap-20181221-0005/
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://php.net/downloads.php
URL	https://bugs.php.net/bug.php?id=77177

PHP var_unserializer.c 'object_common1' Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The object_common1 function in ext/standard/var_unserializer.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via crafted serialized data that is mishandled in a finish_nested_data call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10161
BUGTRAQ	http://www.securityfocus.com/bid/95768

Type	Reference
URL	https://www.tenable.com/security/tns-2017-04
URL	https://github.com/php/php-src/commit/16b3003ffc6393e250f069aa28a78dc5a2c064b2
URL	https://cwe.mitre.org/data/definitions/125.html
URL	https://bugs.php.net/bug.php?id=73825
URL	http://php.net/ChangeLog-5.php
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	http://php.net/ChangeLog-7.php

PHP 'virtual_file_ex' Stack Buffer Overflow — Medium

Vulnerability Details

Integer overflow in the virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-6289
BUGTRAQ	http://www.securityfocus.com/bid/92074
URL	https://support.apple.com/HT207170
URL	http://fortiguard.com/advisory/fortinet-discovers-php-stack-based-buffer-overflow-vulnerabilities

Type	Reference
URL	http://php.net/ChangeLog-7.php
URL	http://git.php.net/?p=php-src.git;a=commit;h=0218acb7e756a469099c4ccfb22bce6c2bd1ef87
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/72513
URL	https://cwe.mitre.org/data/definitions/190.html

PHP 'wddx.c' PDORow String Denial of Service — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/wddx/wddx.c in PHP before 5.6.28 and 7.x before 7.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted serialized data in a wddxPacket XML document, as demonstrated by a PDORow string.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-9934
BUGTRAQ	http://www.securityfocus.com/bid/94845
URL	http://www.php.net/ChangeLog-7.php
URL	https://github.com/php/php-src/commit/6045de69c7dedcba3eadf7c4bba424b19c81d00d
URL	https://bugs.php.net/bug.php?id=73331
URL	https://cwe.mitre.org/data/definitions/476.html

PHP wddx.c 'php_wddx_pop_element' NULL Pointer Dereference Denial of Service Vulnerability

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The php_wddx_pop_element function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid base64 binary value, as demonstrated by a wddx_deserialize call that mishandles a binary element in a wddxPacket XML document.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7130
BUGTRAQ	http://www.securityfocus.com/bid/92764
URL	https://www.tenable.com/security/tns-2016-19
URL	https://github.com/php/php-src/commit/698a691724c0a949295991e5df091ce16f899e02?w=1
URL	https://bugs.php.net/bug.php?id=72750
URL	http://www.php.net/ChangeLog-7.php
URL	https://cwe.mitre.org/data/definitions/476.html

PHP wddx.c 'php_wddx_push_element' Denial of Service

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service (invalid pointer access and out-of-bounds read) or possibly have unspecified other impact via an incorrect boolean element in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7418
BUGTRAQ	http://www.securityfocus.com/bid/93011
URL	https://bugs.php.net/bug.php?id=73065
URL	https://github.com/php/php-src/commit/c4cca4c20e75359c9a13a1f9a36cb7b4e9601d29?w=1
URL	http://www.php.net/ChangeLog-7.php
URL	https://www.tenable.com/security/tns-2016-19
URL	https://cwe.mitre.org/data/definitions/119.html

PHP wddx.c 'wddx_deserialize' NULL Pointer Dereference Denial of Service Vulnerability

Medium

Vulnerability Details

ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via a malformed wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a tag that lacks a < (less than) character.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7131
BUGTRAQ	http://www.securityfocus.com/bid/92768
URL	https://www.tenable.com/security/tns-2016-19
URL	https://cwe.mitre.org/data/definitions/476.html
URL	https://bugs.php.net/bug.php?id=72790
URL	https://github.com/php/php-src/commit/a14fdb9746262549bbbb96abb87338bacd147e1b?w=1
URL	http://www.php.net/ChangeLog-7.php

PHP wddx.c 'wddx_deserialize' NULL Pointer Dereference Denial of Service Vulnerability

Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a stray element inside a boolean element, leading to incorrect pop processing.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7132
BUGTRAQ	http://www.securityfocus.com/bid/92767
URL	https://github.com/php/php-src/commit/a14fdb9746262549bbbb96abb87338bacd147e1b?w=1
URL	https://cwe.mitre.org/data/definitions/476.html

Type	Reference
URL	https://www.tenable.com/security/tns-2016-19
URL	https://bugs.php.net/bug.php?id=72799
URL	http://www.php.net/ChangeLog-7.php

PHP wddx.c XML Deserialization Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

In PHP before 5.6.31, an invalid free in the WDDX deserialization of boolean parameters could be used by attackers able to inject XML for deserialization to crash the PHP interpreter, related to an invalid free for an empty boolean element in ext/wddx/wddx.c.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11143
BUGTRAQ	http://www.securityfocus.com/bid/99553
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	https://www.tenable.com/security/tns-2017-12
URL	https://bugs.php.net/bug.php?id=74145
URL	https://git.php.net/?p=php-src.git;a=commit;h=2aae60461c2ff7b7fbcdd194c789ac841d0747d7
URL	http://php.net/ChangeLog-5.php
URL	http://openwall.com/lists/oss-security/2017/07/10/6

PHP WSDL Injection Attack Vulnerability — Medium

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

The default soap.wsdl_cache_dir setting in (1) php.ini-production and (2) php.ini-development in PHP through 5.6.7 specifies the /tmp directory, which makes it easier for local users to conduct WSDL injection attacks by creating a file under /tmp with a predictable filename that is used by the get_sdl function in ext/soap/php_sdl.c.
Impact:
An attacker can exploit this issue to perform certain unauthorized actions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.6

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-6501
BUGTRAQ	http://www.securityfocus.com/bid/72530
URL	http://php.net/downloads.php
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1009103
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html

PHP 'xmlrpc_decode()' Memory Over-Read Vulnerability — Medium

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of PHP.

Vulnerability Details

An issue was discovered in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1. xmlrpc_decode() can allow a hostile XMLRPC server to cause PHP to read memory outside of allocated areas in base64_decode_xmlrpc in ext/xmlrpc/libxmlrpc/base64.c.
Impact:
Successfully exploiting these issues allow attackers to execute arbitrary code in the affected asset or obtain sensitive information. Failed exploits will result in denial-of-service conditions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-9024
BUGTRAQ	http://www.securityfocus.com/bid/107156
URL	https://security.netapp.com/advisory/ntap-20190321-0001/
URL	http://php.net/downloads.php
URL	https://cwe.mitre.org/data/definitions/125.html
URL	https://bugs.php.net/bug.php?id=77380

PHP XMLRPC Extension Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) via (1) a crafted first argument to the xmlrpc_set_type function or (2) a crafted argument to the xmlrpc_decode function, related to an out-of-bounds read operation.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3668
BUGTRAQ	http://www.securityfocus.com/bid/70666

Type	Reference
URL	http://git.php.net/?p=php-src.git;a=commit;h=88412772d295ebf7dd34409534507dc9bcac726e
URL	http://php.net/ChangeLog-5.php
URL	https://support.apple.com/HT204659
URL	http://linux.oracle.com/errata/ELSA-2014-1767.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1154503
URL	https://bugs.php.net/bug.php?id=68027
URL	http://linux.oracle.com/errata/ELSA-2014-1768.html
URL	https://cwe.mitre.org/data/definitions/119.html

PHP xsltprocessor.c 'xsl_ext_function_php' Denial of Service During Initial Error Checking

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation during initial error checking, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6838.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6837
BUGTRAQ	http://www.securityfocus.com/bid/76738
URL	http://php.net/ChangeLog-5.php

Type	Reference
URL	https://bugs.php.net/bug.php?id=69782

PHP xsltprocessor.c 'xsl_ext_function_php' Denial of Service During Principal Argument Loop — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6837.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6838
BUGTRAQ	http://www.securityfocus.com/bid/76733
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=69782

PHP Zend Denial of Service Vulnerability — Medium

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only relevant for PHP applications that accept untrusted input

(instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.
Impact:
An attacker could cause a denial of service state on the target.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-11628
BUGTRAQ	http://www.securityfocus.com/bid/99489
URL	http://git.php.net/?p=php-src.git;a=commit;h=5f8380d33e648964d2d5140f329cf2d4c443033c
URL	http://git.php.net/?p=php-src.git;a=commit;h=05255749139b3686c8a6a58ee01131ac0047465e
URL	https://bugs.php.net/bug.php?id=74603
URL	http://php.net/downloads.php
URL	https://security.netapp.com/advisory/ntap-20180112-0001/
URL	https://cwe.mitre.org/data/definitions/119.html

PHP zend_exceptions.c Crafted Exception Object Denial of Service — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Zend/zend_exceptions.c in PHP, possibly 5.x before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (infinite loop) via a crafted Exception object in serialized data, a related issue to CVE-2015-8876.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-7478
BUGTRAQ	http://www.securityfocus.com/bid/95150
URL	http://blog.checkpoint.com/2016/12/27/check-point-discovers-three-zero-day-vulnerabilities-web-programming-language-php-7
URL	http://blog.checkpoint.com/wp-content/uploads/2016/12/PHP_Technical_Report.pdf
URL	https://bugs.php.net/bug.php?id=73093
URL	https://security.netapp.com/advisory/ntap-20180112-0001/

PHP 'ZipArchive::extractTo' Function Directory Traversal — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Directory traversal vulnerability in the ZipArchive::extractTo function in ext/zip/php_zip.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 and ext/zip/ext_zip.cpp in HHVM before 3.12.1 allows remote attackers to create arbitrary empty directories via a crafted ZIP archive.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-9767
BUGTRAQ	http://www.securityfocus.com/bid/76652
URL	http://php.net/ChangeLog-5.php
URL	https://github.com/facebook/hhvm/commit/65c95a01541dd2fbc9c978ac53bed235b5376686

Type	Reference
URL	https://bugs.php.net/bug.php?id=70350
URL	https://bugs.php.net/bug.php?id=67996
URL	https://cwe.mitre.org/data/definitions/22.html

PHP zip.c 'phar_parse_zipfile' Denial of Service — Medium

Vulnerability Details

Off-by-one error in the phar_parse_zipfile function in ext/phar/zip.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (uninitialized pointer dereference and application crash) by including the / filename in a .zip PHAR archive.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-7804
BUGTRAQ	http://www.securityfocus.com/bid/76959
URL	http://git.php.net/?p=php-src.git;a=commit;h=1ddf72180a52d247db88ea42a3e35f824a8fbda1
URL	https://support.apple.com/HT205637
URL	https://bugs.php.net/bug.php?id=70433

Ruby 'Oniguruma-mod' and PHP 'mbstring' forward_search_range Denial of Service — Medium

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A SIGSEGV occurs in left_adjust_char_head() during regular expression compilation. Invalid handling of reg->dmax in forward_search_range() could result in an invalid pointer dereference, normally as an immediate denial-of-service condition.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9229
URL	https://github.com/kkos/oniguruma/commit/b690371bbf97794b4a1d3f295d4fb9a8b05d402d
URL	https://cwe.mitre.org/data/definitions/476.html
URL	https://github.com/kkos/oniguruma/issues/59

Samba 'before 4.7.3' Possible Remote Sensitive Information Access Vulnerability

Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear allocated heap memory.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-15275

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/101908
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://www.synology.com/support/security/Synology_SA_17_72_Samba
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03817en_us
URL	https://www.samba.org/samba/security/CVE-2017-15275.html

Samba Confidential Attribute Values Disclosure Vulnerability — Medium

Solution Details

Please upgrade to the most current stable release of Samba, available at http://www.samba.org.
Workarounds:
The only workaround is not to use the SEARCH_FLAG_CONFIDENTIAL
searchFlags bit, not to expect confidentiality of the attribute list
above nor to set access control entries of a similar nature on LDAP
objects.

Vulnerability Details

The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4

CVSS Vector: AV:N/AC:L/Au:S/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10919
BUGTRAQ	http://www.securityfocus.com/bid/105081
URL	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10919
URL	https://www.samba.org/samba/security/CVE-2018-10919.html
URL	https://nvd.nist.gov/vuln/detail/CVE-2018-10919

Type	Reference
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://security.netapp.com/advisory/ntap-20180814-0001/
URL	https://www.samba.org/samba/history/security.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10919

Samba 'DelegationNotAllowed' Vulnerability — Medium

Vulnerability Details

The DelegationNotAllowed Kerberos feature restriction was not being applied when processing protocol transition requests (S4U2Self), in the AD DC KDC.
Impact:
Samba server fails to honor user attributes for S4USelf even if set on client.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Samba.

CVSS Base Score: 6.4

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-14870
URL	https://wiki.samba.org/index.php/Updating_Samba

Samba 'dirsync' Denial of Service Vulnerability — Medium

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Samba.

Vulnerability Details

A flaw was found in Samba where an attacker can crash AD DC LDAP server via dirsync resulting in denial of service. Privilege escalation is not possible with this issue.
Impact:
An attacker can exploit this vulnerability to cause a denial-of-service condition, denying service to legitimate users.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4

CVSS Vector: AV:N/AC:L/Au:S/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-14847
URL	https://wiki.samba.org/index.php/Updating_Samba

Samba 'DNS' Denial of Service Vulnerability — Medium

Vulnerability Details

An authenticated user can crash the DCE/RPC DNS management server by creating records with a matching zone name.
Impact:
An attacker can exploit this vulnerability to cause a denial-of-service condition, denying service to legitimate users.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Samba.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 3.5

CVSS Vector: AV:N/AC:M/Au:S/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-14861
URL	https://wiki.samba.org/index.php/Updating_Samba

Samba Incorrect 'KDC' Implementation Vulnerability — Medium

Vulnerability Details

The checksum validation in the S4U2Self handler in the embedded Heimdal KDC did not first confirm that the checksum was keyed, allowing replacement of the requested target (client) principal.
Impact:

An attacker could leverage this vulnerability to bypass certain security restrictions and perform unauthorized actions by conducting a man-in-the-middle attack.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Samba.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6

CVSS Vector: AV:N/AC:M/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-16860
URL	http://www.samba.org/samba/security/
URL	https://wiki.samba.org/index.php/Updating_Samba

Samba Input Validation Vulnerability — Medium

Solution Details

Please upgrade to the most current stable release of Samba, available at http://www.samba.org.

Vulnerability Details

A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.5

CVSS Vector: AV:N/AC:L/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10858
BUGTRAQ	http://www.securityfocus.com/bid/105085
URL	https://security.netapp.com/advisory/ntap-20180814-0001/
URL	https://cwe.mitre.org/data/definitions/119.html

Type	Reference
URL	https://www.samba.org/samba/security/CVE-2018-10858.html
URL	https://nvd.nist.gov/vuln/detail/CVE-2018-10858
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-10858
URL	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10858
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10284
URL	https://www.samba.org/samba/history/security.html

Samba 'KDC' Denial of Service Vulnerability — Medium

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of Samba.

Vulnerability Details

Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.
Impact:
An attacker can exploit this issue to cause the application to crash, denying service to legitimate users.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4

CVSS Vector: AV:N/AC:L/Au:S/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-16841
BUGTRAQ	http://www.securityfocus.com/bid/106023
URL	https://www.samba.org/samba/security/CVE-2018-16841.html
URL	https://wiki.samba.org/index.php/Updating_Samba
URL	https://security.netapp.com/advisory/ntap-20181127-0001/

Type	Reference
URL	https://cwe.mitre.org/data/definitions/415.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-16841

Samba Kerberos Impersonation Vulnerability — Medium

Vulnerability Details

It was found that Samba before versions 4.5.3, 4.4.8, 4.3.13 always requested forwardable tickets when using Kerberos authentication. A service to which Samba authenticated using Kerberos could subsequently use the ticket to impersonate Samba to other services or domain users.
Impact:
An attacker can exploit this issue to impersonate arbitrary users and perform unauthorized actions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please upgrade to the most current stable release of Samba, available at https://wiki.samba.org/index.php/Updating_Samba

CVSS Base Score: 3.3

CVSS Vector: AV:A/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2125
BUGTRAQ	http://www.securityfocus.com/bid/94988
URL	https://cwe.mitre.org/data/definitions/20.html
URL	https://www.samba.org/samba/security/CVE-2016-2125.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-2125

Samba 'LDAP' Search Denial of Service Vulnerability — Medium

Vulnerability Details

Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the

process. There is no further vulnerability associated with this issue, merely a denial of service.
Impact:
An attacker can exploit this issue to cause the application to crash, denying service to legitimate users.

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of Samba.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4

CVSS Vector: AV:N/AC:L/Au:S/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-16851
BUGTRAQ	http://www.securityfocus.com/bid/106027
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-16851
URL	https://www.samba.org/samba/security/CVE-2018-16851.html
URL	https://security.netapp.com/advisory/ntap-20181127-0001/
URL	https://cwe.mitre.org/data/definitions/476.html
URL	https://wiki.samba.org/index.php/Updating_Samba

Samba 'LDAP' Server Denial of Service Vulnerability — Medium

Vulnerability Details

A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.
Impact:
An attacker can exploit this issue to cause the application to crash, denying service to legitimate users.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to External References for a link to upgrade to the most recent stable version of Samba.

CVSS Base Score: 4

CVSS Vector: AV:N/AC:L/Au:S/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-14629
BUGTRAQ	http://www.securityfocus.com/bid/106022
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-14629
URL	https://www.samba.org/samba/security/CVE-2018-14629.html
URL	https://security.netapp.com/advisory/ntap-20181127-0001/
URL	https://wiki.samba.org/index.php/Updating_Samba
URL	https://cwe.mitre.org/data/definitions/400.html

Samba Man in the Middle Hijack Vulnerability — Medium

Solution Details

Please upgrade to the most current stable release of Samba, available at http://www.samba.org.
Workarounds:
The missing implied signing for 'smb2mount -e', 'smbcacls -e' and 'smbcquotas -e' can be enforced by explicitly using '--signing=required' on the commandline or "client signing = required" in smb.conf.

Vulnerability Details

It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12150
BUGTRAQ	http://www.securityfocus.com/bid/100918
URL	https://www.samba.org/samba/security/CVE-2017-12150.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-12150

Type	Reference
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbns03775en_us
URL	https://security.netapp.com/advisory/ntap-20170921-0001/
URL	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12150
URL	https://nvd.nist.gov/vuln/detail/CVE-2017-12150
URL	https://www.samba.org/samba/history/security.html
URL	https://cwe.mitre.org/data/definitions/254.html
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03817en_us

Samba Man in the Middle Vulnerability — Medium

Solution Details

Please upgrade to the most current stable release of Samba, available at http://www.samba.org.
Workarounds:
Keep the default of "client max protocol = NT1".

Vulnerability Details

A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12151
BUGTRAQ	http://www.securityfocus.com/bid/100917
URL	https://nvd.nist.gov/vuln/detail/CVE-2017-12151
URL	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12151

Type	Reference
URL	https://cwe.mitre.org/data/definitions/310.html
URL	https://www.samba.org/samba/security/CVE-2017-12151.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-12151
URL	https://www.samba.org/samba/history/security.html
URL	https://security.netapp.com/advisory/ntap-20170921-0001/
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03817en_us

Samba 'ndr_pull_dnsp_name' Remote Privilege Escalation Vulnerability — Medium

Vulnerability Details

A flaw was found in samba versions 4.0.0 to 4.5.2. The Samba routine ndr_pull_dnsp_name contains an integer wrap problem, leading to an attacker-controlled memory overwrite. ndr_pull_dnsp_name parses data from the Samba Active Directory ldb database. Any user who can write to the dnsRecord attribute over LDAP can trigger this memory corruption. By default, all authenticated LDAP users can write to the dnsRecord attribute on new DNS objects. This makes the defect a remote privilege escalation.
Impact:
An attacker can exploit this issue to execute arbitrary code in the context of the affected application. Failed exploit attempts will likely result in a denial of service.

Solution Details

Please upgrade to the most current stable release of Samba, available at https://wiki.samba.org/index.php/Updating_Samba

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.5

CVSS Vector: AV:N/AC:L/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2123
BUGTRAQ	http://www.securityfocus.com/bid/94970
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-2123

Type	Reference
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://www.samba.org/samba/security/CVE-2016-2123.html

Samba November 2021 Security Update — Medium

Solution Details

Please upgrade to the latest version of Samba or patch your system (if applicable).

Samba 4.15.2, 4.14.10 and 4.13.14 have been issued as security releases to correct the defect. Samba vendors and administrators running affected versions are advised to upgrade or apply the patch as soon as possible.

For potential patches: https://www.samba.org/samba/security/

Vulnerability Details

There are several vulnerabilities resolved ranging from fragment injection to use after free vulnerabilities and privilege escalation. It is recommended to update Samba to the latest version to avoid exploitation. CVE-2020-25717, a user in an AD domain could become root on domain members.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9

CVSS Vector: AV:N/AC:L/Au:S/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2124
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25717
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25719
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25718
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25722
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-3738
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-23192
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-25721

Type	Reference
URL	https://ubuntu.com/security/CVE-2016-2124
URL	https://access.redhat.com/security/cve/cve-2020-25719
URL	https://www.suse.com/security/cve/CVE-2020-25718.html
URL	https://bugzilla.samba.org/show_bug.cgi?id=12444
URL	https://www.samba.org/samba/security/CVE-2020-25717.html
URL	https://www.samba.org/samba/history/security.html

Samba 'PAC' Checksum Denial of Service Vulnerability — Medium

Solution Details

Please upgrade to the most current stable release of Samba, available at
https://wiki.samba.org/index.php/Updating_Samba

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Samba version 4.0.0 up to 4.5.2 is vulnerable to privilege elevation due to incorrect handling of the PAC (Privilege Attribute Certificate) checksum. A remote, authenticated, attacker can cause the winbindd process to crash using a legitimate Kerberos ticket. A local service with access to the winbindd privileged pipe can cause winbindd to cache elevated access permissions.
Impact:
An attacker can exploit this issue to cause the application to crash the winbindd process, denying service to legitimate users.

CVSS Base Score: 4

CVSS Vector: AV:N/AC:L/Au:S/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2126
BUGTRAQ	http://www.securityfocus.com/bid/94994
URL	https://www.samba.org/samba/security/CVE-2016-2126.html
URL	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA43730

Samba Password Change Vulnerability — Medium

Solution Details

Please upgrade to the most current stable release of Samba, available at http://www.samba.org.
Workarounds:
Possible workarounds are described at a dedicated page in the Samba wiki:

https://wiki.samba.org/index.php/CVE-2018-1057

Vulnerability Details

On a Samba 4 AD DC the LDAP server in all versions of Samba from 4.0.0 onwards incorrectly validates permissions to modify passwords over LDAP allowing authenticated users to change any other users' passwords, including administrative users and privileged service accounts (eg Domain Controllers).

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.5

CVSS Vector: AV:N/AC:L/Au:S/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1057
URL	http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1057
URL	https://security.netapp.com/advisory/ntap-20180313-0001/
URL	https://www.samba.org/samba/security/CVE-2018-1057.html
URL	https://www.samba.org/samba/history/security.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1553553
URL	http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1057
URL	https://cwe.mitre.org/data/definitions/275.html
URL	https://www.synology.com/support/security/Synology_SA_18_08

Samba Registry Hive File Creation Vulnerability — Medium

Vulnerability Details

A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before

4.8.11, 4.9.6 and 4.10.2 are vulnerable.
Impact:
Authenticated attackers with write permissions could leverage this vulnerability to trigger a symlink traversal to write or detect files outside the Samba share.

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Samba.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.5

CVSS Vector: AV:N/AC:L/Au:S/C:N/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-3880
URL	https://support.f5.com/csp/article/K20804356
URL	https://cwe.mitre.org/data/definitions/22.html
URL	https://www.synology.com/security/advisory/Synology_SA_19_15
URL	https://security.netapp.com/advisory/ntap-20190411-0004/
URL	https://access.redhat.com/security/cve/cve-2019-3880
URL	https://www.samba.org/samba/security/CVE-2019-3880.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-3880
URL	https://wiki.samba.org/index.php/Updating_Samba

Samba Server Memory Information Leak over SMB1 — Medium

Solution Details

Please upgrade to the most current stable release of Samba, available at http://www.samba.org.
Workarounds:
As this is an SMB1-only vulnerability, it can be avoided by setting
the server to only use SMB2 via adding:

server min protocol = SMB2_02

to the [global] section of your smb.conf and restarting smbd.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.

CVSS Base Score: 4.8

CVSS Vector: AV:A/AC:L/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-12163
BUGTRAQ	http://www.securityfocus.com/bid/100925
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03817en_us
URL	https://security.netapp.com/advisory/ntap-20170921-0001/
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2017-12163
URL	https://www.samba.org/samba/security/CVE-2017-12163.html
URL	https://nvd.nist.gov/vuln/detail/CVE-2017-12163
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbns03775en_us
URL	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12163
URL	https://www.samba.org/samba/history/security.html
URL	https://www.synology.com/support/security/Synology_SA_17_57_Samba

Samba 'smbXcli_base.c' Man-In-The-Middle Client-Signing Protection Bypass — Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

libcli/smb/smbXcli_base.c in Samba 4.x before 4.2.14, 4.3.x before 4.3.11, and 4.4.x before 4.4.5 allows man-in-the-middle attackers to bypass a client-signing protection mechanism, and consequently spoof SMB2 and SMB3 servers, via the (1) SMB2_SESSION_FLAG_IS_GUEST or (2) SMB2_SESSION_FLAG_IS_NULL flag.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2119
BUGTRAQ	http://www.securityfocus.com/bid/91700
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinjul2016-3090544.html
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://www.samba.org/samba/security/CVE-2016-2119.html

Samba Symlink Denial of Service — Medium

Vulnerability Details

smbd in Samba before 4.4.10 and 4.5.x before 4.5.6 has a denial of service vulnerability (fd_open_atomic infinite loop with high CPU usage and memory consumption) due to wrongly handling dangling symlinks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:L/Au:S/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-9461

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/99455
URL	https://bugs.debian.org/864291
URL	https://bugzilla.samba.org/show_bug.cgi?id=12572
URL	https://cwe.mitre.org/data/definitions/399.html
URL	https://git.samba.org/?p=samba.git;a=commit;h=10c3e3923022485c720f322ca4f0aca5d7501310

Samba Unauthorized File Creation Vulnerability — Medium

Solution Details

Refer to the External References for a link to upgrade to the most recent stable version of Samba.

Vulnerability Details

A flaw was found in the samba where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames.
Impact:
An attacker could leverage this vulnerability to create files outside of the current working directory using the privileges of the client user.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-10218
URL	https://www.samba.org/samba/security/CVE-2019-10218.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2019-10218
URL	https://wiki.samba.org/index.php/Updating_Samba

Slowloris Resource Depletion And Denial Of Service — Medium

False Positive Notes

This item may be a false positive under certain conditions or if a backported solution has been applied. Please validate and document remediation efforts through Active View.

Solution Details

This attack can be mitigated by; 1) limiting the number of inactive concurrent web server connections a single user may be allowed to maintain, or 2) setting a minimum threshold of data per second a web server connection is allowed to maintain without being dropped.

Examples of applicable apache modules useful for implementing suggested remediation include:
mod_reqtimeout - http://httpd.apache.org/docs/2.3/mod/mod_reqtimeout.html
mod_qos - http://sourceforge.net/projects/mod-qos/
mod_cband - http://cband.linux.pl
mod_limitpconn - http://dominia.org/djao/limitipconn.html
mod_evasive - http://www.networkdweebs.com/stuff/security.html
mod_security - http://www.modsecurity.org/
mod_antiloris - ftp://ftp.monshouwer.eu/pub/linux/mod_antiloris/

Additional third party modules may also be available. Please contact the vendor for additional information.

Vulnerability Details

This host is running a web server that appears to utilize a configuration which allows a single remote host to consume all connection resources. The slowloris denial of service is achieved by systematically establishing and maintaining connections through partial header requests and http keepalive messages. The attacker can continue this methodology until all web server connections are tied up, resulting in a complete denial of service to legitimate users. Web servers that utilize threading are more susceptible to a slowloris attack. In contrast to other web server denial of service techniques, this attack only requires a tiny amount of bandwidth and a single host IP address.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6750
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5568
BUGTRAQ	http://www.securityfocus.com/bid/56686
BUGTRAQ	http://www.securityfocus.com/bid/21865
URL	https://cwe.mitre.org/data/definitions/16.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=880011
URL	http://www.howtoforge.com/how-to-defend-slowloris-ddos-with-mod_qos-apache2-on-debian-lenny

Type	Reference
URL	http://captainholly.wordpress.com/2009/06/19/slowloris-vs-tomcat/
URL	http://wiki.apache.org/httpd/DoS
URL	https://cwe.mitre.org/data/definitions/399.html
URL	http://www.apachelounge.com/viewtopic.php?t=3137
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05158380
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05111017

SMB Writeable Directories — Medium

Vulnerability Details

The remote host has SMB sharing enabled and contains directories which are writeable by anonymous users. A malicious user can leverage this capability in order to create, modify or delete files. Possible attack scenarios include the creation of malicious executables or falsified information that is now trusted by legitimate users of the system.

Solution Details

If it is unnecessary for anonymous users to have write privileges on the vulnerable SMB directories, consider disabling write privileges or completely revoking anonymous access. Running services with unnecessary privileges gives malicious users a larger attack surface.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.4

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N

Type	Reference
There are no references for this vulnerability.	

SNMP Default Communities — Medium

Solution Details

Disable SNMP on this host unless it is specifically required for remote management purposes. If SNMP is required, change the SNMP community strings to be complex and difficult for an attacker to guess.

Some sample methods for changing SNMP community strings on common platforms have been provided below. For specific instructions, please consult this host's user manual or contact the vendor of this host for assistance.

Cisco routers:
In Enable mode, type:
'snmp-server community ' to add a specified community string.
'no snmp-server community ' to remove a specified community string.
'no snmp-server' to disable the SNMP server.

HP JetDirect:
The read-only community strings of 'public' and 'internal' can not be changed. These strings are used by the JetAdmin software, and are hard coded into the firmware. Please contact HP directly to find out how to properly secure a HP Printer. It is possible to change the write community string by typing the following via a TELNET session:
set-cmnty-name: NewString
The only valid workaround for this vulnerability on a HP JetDirect printer is to disable SNMP using the following command via TELNET:
snmp-config: 0

Without SNMP, the Embedded WebServer will not function properly, so it is recommended that EWS be disabled using the following command via TELNET: ews-config: 0
SNMP can be disabled in more recent versions of the JetDirect firmware. If this command is not available, please upgrade the printer firmware to the latest available.
Caveats:
In certain devices the SNMP community strings are read-only and thus cannot be changed. In these situations, contact the vendor for the proper procedure to secure the device.

Additionally, changing the SNMP community string will affect management tools which utilize SNMP to remotely manage this host. Please ensure that any such tools have are reconfigured accordingly.
Workarounds:
In some situations, the SNMP community strings are not user configurable. In those cases, utilize other means such as host or network based firewall rules to restrict access to authorized hosts only.

Vulnerability Details

Simple Network Management Protocol is a protocol designed for managing and monitoring network devices such as routers, switches, workstations, and more. SNMP versions 1 and 2 support authentication using "community strings" which is similar to a password which grants access to specific roles based on the community string provided. Most vendors ship devices with pre-defined SNMP community strings for read access and for write access to the device. For example, many vendors use "public" as the pre-configure read only community string.

Attackers use lists of default and well known community strings in combination with brute force attacks to attempt to gain read or read/write access to the devices via SNMP.
Impact:
An attacker can leverage default community strings to manage the remote host. Based on the supplied community string, the attacker will have specific permissions to perform certain tasks. In some cases,

the attacker may only be able to read device statistics and configurations. Given a more privileged community string, an attacker may be able to change the configuration of the device or cause it to take certain actions such as reboot or shut down.

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0517

SSH Accepts Any Login — Medium

Solution Details

Please disable this SSH server or reconfigure it to not accept arbitrary username and password combinations.

Vulnerability Details

The SSH Server on this host appears to accept any username/password combination as valid. On some SSH servers, this can indicate that a blank username/password combination is considered to be valid by the host system. An attacker can leverage this to gain access to or information about this host.

False Positive Notes

Some SSH servers can behave abnormally or in an unexpected manner. This can give the appearance that the server is accepting any username/password combination as correct.

It is recommended that SSH logins be manually tested to verify their accuracy. There are cases where the abnormal behavior can cause a False Positive.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:M/Au:N/C:C/I:C/A:C

Type	Reference
There are no references for this vulnerability.	

Threat Scan: Antivirus Software Not Installed — Medium

Solution Details

Please install an antivirus product on this asset.

Vulnerability Details

This asset does not appear to be running any antivirus software. Security industry best practices dictate that Windows machines have antivirus software protections in place.

False Positive Notes

See the data section of this vulnerability for more information on the antivirus products checked. If this asset has an antivirus product installed that is not on this list, then this vulnerability may be a false positive.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Threat Scan: McAfee VirusScan Enterprise Definitions Outdated — Medium

Vulnerability Details

The McAfee VirusScan Enterprise antivirus signatures on this asset are over two weeks old.
Impact:
Outdated antivirus definitions may prevent McAfee VirusScan Enterprise from detecting the latest threats that McAfee has written a definition for.

Solution Details

Update to the latest set of antivirus definitions from McAfee.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Threat Scan: McAfee VirusScan Enterprise Disabled — Medium

Solution Details

Enable McAfee VirusScan Enterprise.

Vulnerability Details

McAfee VirusScan Enterprise is installed on this asset, but it is currently disabled.
Impact:

While McAfee VirusScan Enterprise is disabled, this asset is at an increased risk of being infected with malware.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Threat Scan: Unsigned Software Processes — Medium

Solution Details

The detection of unsigned software running does not necessarily indicate that this software is malicious. Nevertheless, steps should be taken to determine that any detected unsigned software is not malicious. Additionally, if the software is published by a well-known vendor, requests should be made to the vendor to ask that only digitally-signed software is provided.

Vulnerability Details

This asset has one or more processes running that are backed by images that are unsigned. Digital signatures provide a measure of trust that a piece of software came from a specific vendor and that it was not altered after it was published. The majority of malware that executes from an image on disk will not be signed. This detection does not guarantee that the reported unsigned software is malicious, but rather provides a list of items that should be examined closer to determine that they are not malicious. Additionally, best practices suggest that only signed software should run on Windows endpoints.
Impact:
Unsigned software can pose several risks. One is that if you run unsigned software that was downloaded from the Internet, there is a chance that it could have been tampered with if the connection was not encrypted. Additionally, there is no guarantee that it hasn't been tampered with since it was downloaded. An attacker may have gained access to the endpoint and overwritten the binary with their own, or otherwise introduced a backdoor. Software that is digitally signed cannot be tampered with in this way without invalidating the signature and thus alerting you to the fact that the software is not in its original published form.

False Positive Notes

Please note that it is possible that a false positive could occur if the endpoint being scanned is running Windows Vista, Server 2008, or Server 2008 R2 and the file was signed using the Sha-256 algorithm. These versions of Windows have limited support for Sha-256 and expect files to be signed using Sha-1. For example, Frontline uses a Sha-256 algorithm to sign it's binary used to gather threat data. As a result, it may show up in the list of unsigned software processes on these Windows versions, even though it is actually signed.

It is possible to apply a hotfix to add support for Sha-256. To do so, please reference the DigiCert link in the external references section for this vulnerability.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://en.wikipedia.org/wiki/Code_signing
URL	https://knowledge.digicert.com/generalinformation/INFO3199.html

Threat Scan: Windows Defender Definitions Outdated — Medium

Vulnerability Details

The Windows Defender antivirus signatures on this asset are over two weeks old.
Impact:
Outdated antivirus definitions may prevent Windows Defender from detecting the latest threats that Microsoft has written a definition for.

Solution Details

Run "Check for updates" to get the latest definitions from Microsoft.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Threat Scan: Windows Defender Disabled — Medium

Vulnerability Details

Windows Defender is not enabled on this asset.
Impact:
While Windows Defender is disabled, this asset is at an increased risk of being infected with malware.

Solution Details

Enable Windows Defender.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

VMware Security Advisory: VMSA-2018-0012 — Medium

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

CVSS Base Score: 2.1

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-3639
BUGTRAQ	http://www.securityfocus.com/bid/104232
URL	https://security.netapp.com/advisory/ntap-20180521-0001/
URL	https://www.vmware.com/security/advisories/VMSA-2018-0012.html
URL	http://support.lenovo.com/us/en/solutions/LEN-22133
URL	https://support.citrix.com/article/CTX235225
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-268644.pdf
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03850en_us

Type	Reference
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180012
URL	https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
URL	http://xenbits.xen.org/xsa/advisory-263.html
URL	https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-18-0006
URL	https://bugs.chromium.org/p/project-zero/issues/detail?id=1528
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0004
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-505225.pdf
URL	http://www.fujitsu.com/global/support/products/software/security/products-f/cve-2018-3639e.html
URL	https://developer.arm.com/support/arm-security-updates/speculative-processor-vulnerability
URL	https://www.synology.com/support/security/Synology_SA_18_23
URL	https://nvidia.custhelp.com/app/answers/detail/a_id/4787
URL	https://support.oracle.com/knowledge/Sun%20Microsystems/2481872_1.html
URL	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00115.html

VMware Security Advisory: VMSA-2018-0016 | Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.1

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6965
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6966
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6967
BUGTRAQ	http://www.securityfocus.com/bid/104709
URL	https://cwe.mitre.org/data/definitions/125.html
URL	https://www.vmware.com/security/advisories/VMSA-2018-0016.html
URL	https://www.vmware.com/security/advisories/VMSA-2018-0016.html

VMware Security Advisory: VMSA-2018-0018 — Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.5

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6972
BUGTRAQ	http://www.securityfocus.com/bid/104884
URL	https://cwe.mitre.org/data/definitions/476.html

Type	Reference
URL	https://www.vmware.com/security/advisories/VMSA-2018-0018.html
URL	https://www.vmware.com/security/advisories/VMSA-2018-0018.html

VMware Security Advisory: VMSA-2018-0020 Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.7

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-3646
BUGTRAQ	http://www.securityfocus.com/bid/105080
URL	https://cert-portal.siemens.com/productcert/pdf/ssa-254686.pdf
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
URL	https://www.oracle.com/technetwork/security-advisory/cpujan2019-5072801.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://www.synology.com/support/security/Synology_SA_18_45
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&amp;docId=emr_na-hpesbhf03874en_us
URL	https://software.intel.com/security-software-guidance/software-guidance/l1-terminal-fault

Type	Reference
URL	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00161.html
URL	https://foreshadowattack.eu/
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180018
URL	https://support.f5.com/csp/article/K31300402
URL	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2018-0010
URL	http://www.vmware.com/security/advisories/VMSA-2018-0020.html
URL	https://www.vmware.com/security/advisories/VMSA-2018-0020.html
URL	https://security.netapp.com/advisory/ntap-20180815-0001/
URL	http://xenbits.xen.org/xsa/advisory-273.html
URL	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20180815-01-cpu-en
URL	http://support.lenovo.com/us/en/solutions/LEN-24163

VMware Security Advisory: VMSA-2019-0006 Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5520

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5517
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5516
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-369/
URL	https://www.vmware.com/security/advisories/VMSA-2019-0006.html
URL	https://cwe.mitre.org/data/definitions/125.html
URL	https://www.talosintelligence.com/vulnerability_reports/TALOS-2019-0762
URL	https://www.vmware.com/security/advisories/VMSA-2019-0006.html

VMware Security Advisory: VMSA-2019-0008 Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.7

CVSS Vector: AV:L/AC:M/Au:N/C:C/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12126
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12130
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-11091
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12127
URL	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html
URL	https://cwe.mitre.org/data/definitions/200.html

Type	Reference
URL	https://www.vmware.com/security/advisories/VMSA-2019-0008.html

VMware Security Advisory: VMSA-2019-0013 Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.7

CVSS Vector: AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-16544
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5534
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5532
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5531
URL	https://git.busybox.net/busybox/commit/?id=c3797d40a1c57352192c6106cc0f435e7d9c11e8
URL	https://cwe.mitre.org/data/definitions/94.html
URL	https://www.vmware.com/security/advisories/VMSA-2019-0013.html
URL	https://www.twistlock.com/2017/11/20/cve-2017-16544-busybox-autocompletion-vulnerability/

VMware Security Advisory: VMSA-2019-0020 Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.9

CVSS Vector: AV:L/AC:L/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-11135
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-12207
URL	https://www.vmware.com/security/advisories/VMSA-2019-0020.html

VMware Security Advisory: VMSA-2020-0008 Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.3

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3955
URL	https://www.vmware.com/security/advisories/VMSA-2020-0008.html

VMware Security Advisory: VMSA-2020-0012 Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

CVSS Base Score: 8.4

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3960
URL	https://www.vmware.com/security/advisories/VMSA-2020-0012.html

VMware Security Advisory: VMSA-2020-0015 Medium

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

CVSS Base Score: 8.2

CVSS Vector: AV:L/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3963
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3964
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3968

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3967
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3966
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3962
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3969
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3965
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3970
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3971
URL	https://www.vmware.com/security/advisories/VMSA-2020-0015.html

VMware Security Advisory: VMSA-2020-0018 — Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.3

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3976
URL	https://www.vmware.com/security/advisories/VMSA-2020-0018.html
URL	https://www.vmware.com/security/advisories/VMSA-2020-0018.html

VMware Security Advisory: VMSA-2021-0014 — Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 9.8

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21995
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-21994
URL	https://www.vmware.com/security/advisories/VMSA-2021-0014.html

VMware Security Advisory: VMSA-2022-0001 — Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22045
URL	https://www.vmware.com/security/advisories/VMSA-2022-0001.html

VMware Security Advisory: VMSA-2022-0004 Medium

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22041
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22050
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22042
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22040
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-22043
URL	https://www.vmware.com/security/advisories/VMSA-2022-0004.html

Zend Recursive Method Denial of Service Medium

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

Stack consumption vulnerability in Zend/zend_exceptions.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to cause a denial of service (segmentation fault) via recursive method calls.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-8873
URL	https://bugs.php.net/bug.php?id=69793
URL	http://git.php.net/?p=php-src.git;a=commit;h=4d2278143a08b7522de9471d0f014d7357c28fea
URL	http://php.net/ChangeLog-5.php
URL	https://cwe.mitre.org/data/definitions/20.html

Zoom 'Share Screen' Information Disclosure Vulnerability — Medium

Vulnerability Details

Zoom sometimes allows attackers to read private information on a participant's screen, even though the participant never attempted to share the private part of their screen. When a user shares a specific application window via the Share Screen functionality, other meeting participants can briefly see contents of other application windows that were explicitly not shared. The contents of these other windows can be seen for a short period of time when they overlay the shared window and get into focus. (An attacker can, of course, use a separate screen-recorder application, unsupported by Zoom, to save all such contents for later replays and analysis.) Depending on the unintentionally shared data, this short exposure of screen contents may be a more or less severe security issue.
Impact:
An attacker could leverage this vulnerability to obtain sensitive information in the context of the affected asset.

Solution Details

Refer to External References for a link to the most recent stable version of the Zoom client.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-28133
URL	https://zoom.us/download
URL	https://zoom.us/docs/en-us/trust/security/security-bulletin.html

Anonymous FTP Enabled — Low

Solution Details

If this FTP server is no longer required, disable the service from the host. Otherwise, the FTP server should be configured to not allow anonymous logins. This can be accomplished by changing the 'ftp' user in /etc/passwd to 'noftp' or remove it entirely. Also, make sure that the ftp user's home directory is owned by root. For Microsoft, disable anonymous FTP through the IIS Internet Service Manager. In the left windowpane select Console Root ->Internet Information Server ->IIS ->Default FTP Site. Right mouse click and go to Properties. Go to the 'Security Accounts' tab and de-select 'Allow Anonymous Connections'.

Caveats:
Caution should be used when editing a sensitive file such as /etc/passwd. This file controls all user login information for the host. If errors are made, it could prevent any user from logging in to the host.

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

Vulnerability Details

The FTP service on this host is configured to allow anonymous access to the server. Anonymous access allows any user to log in remotely to the server without providing a username and password to authenticate. With anonymous access, a remote attacker could potentially log into the FTP server and upload or download data at will.

Impact:
Anonymous access could be used to harbor malicious files for attackers to use in further attacks on the network, or even across the internet. It can also allow attackers to access any sensitive data that may be stored on an FTP server.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0497

Apache Default Start Page — Low

Vulnerability Details

This host is running Apache web server. The default Apache "It Works!" Page implies this host may not be configured for optimal security. An attacker can leverage this to gain access to or information about this host.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please ensure this host is configured to appropriately restrict access.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Apache HTTP Server mod_cluster Improper Input Validation Vulnerability — Low

Vulnerability Details

Apache HTTP Server mod_cluster before version httpd 2.4.23 is vulnerable to an Improper Input Validation in the protocol parsing logic in the load balancer resulting in a Segmentation Fault in the serving httpd process.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to version 2.4.3 or later.

CVSS Base Score: 4.3

CVSS Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-8612
BUGTRAQ	http://www.securityfocus.com/bid/94939
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1387605
URL	https://security.netapp.com/advisory/ntap-20180601-0005/
URL	https://cwe.mitre.org/data/definitions/20.html

Apache Manual Page Information Leak — Low

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This host reveals an accessible web directory. Attackers can leverage this information to target further attacks.

Solution Details

Remove or unlink the http://<host>/manual/ web directory on this host.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Apache Range Header Denial Of Service — Low

Solution Details

Apache has released version 2.2.20 of the Apache Web Server which addresses this flaw. Apache highly recommends that all users upgrade to this version. Please see the External References section for links to information about this update.

If it is not feasible to upgrade the server due to vendor constraints, several different remediation options have been provided:

1) Use SetEnvIf or mod_rewrite to detect a large number of ranges and then either ignore the Range: header or reject the request.

Option 1: (Apache 2.0 and 2.2)

```
# Drop the Range header when more than 5 ranges.
# CVE-2011-3192
SetEnvIf Range (,.*?){5,} bad-range=1
RequestHeader unset Range env=bad-range

# optional logging.
CustomLog logs/range-CVE-2011-3192.log common env=bad-range
```

Option 2: (Also for Apache 1.3)

```
# Reject request when more than 5 ranges in the Range: header.
# CVE-2011-3192
#
RewriteEngine on
RewriteCond %{HTTP:range} !(^bytes=[^,]+(,[^,]+){0,4}$|^$)
```

RewriteRule .* - [F]

The number 5 is arbitrary. Several 10's should not be an issue and may be required for sites which for example serve PDFs to very high end eReaders or use things such complex http based video streaming.

2) Limit the size of the request field to a few hundred bytes. Note that while this keeps the offending Range header short - it may break other headers; such as sizeable cookies or security fields.

LimitRequestFieldSize 200

Note that as the attack evolves in the field you are likely to have to further limit this and/or impose other LimitRequestFields limits.

See: http://httpd.apache.org/docs/2.2/mod/core.html#limitrequestfieldsize

3) Use mod_headers to completely dis-allow the use of Range headers:

RequestHeader unset Range

Note that this may break certain clients - such as those used for e-Readers and progressive/http-streaming video.

4) Deploy a Range header count module as a temporary stopgap measure:

http://people.apache.org/~dirkx/mod_rangecnt.c

Precompiled binaries for some platforms are available at:

http://people.apache.org/~dirkx/BINARIES.txt

5) Apply any of the current patches under discussion - such as:

http://mail-archives.apache.org/mod_mbox/httpd-dev/201108.mbox/%3cCAAPSnn2PO-d-C4nQt_TES2RRWiZr7urefhTKPWBC1b+K1Dqc7g@mail.gmail.com%3e

Vulnerability Details

The Apache web server running on this host appears to be susceptible to a denial of service condition. Apache versions 1.3.x and 2.x are all vulnerable to malicious requests which attempt to set the Range header with multiple overlapping byte ranges. Under normal conditions, a client may use the Range header to specify the number of bytes to receive a chunk of large data in. When an attacker modifies this to include many different byte ranges, the Apache web server will attempt to process all of them and consume all memory resources which can lead to system instability, process shutdown, and complete denial of service.
Impact:
By opening a moderate amount of connections to the vulnerable Apache web server, an attacker may be able to cause Apache to consume all memory resources on the affected server. This will result in system instability and eventually complete denial of service. This attack does not require the amount of bandwidth that a typical distributed denial of service attack would utilize. Therefore, it is extremely important to resolve this flaw by either upgrading or applying one of the workarounds provided.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.8

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3192
BUGTRAQ	http://www.securityfocus.com/bid/49303
URL	https://bugzilla.redhat.com/show_bug.cgi?id=732928
URL	http://www.oracle.com/technetwork/topics/security/cpujul2012-392727.html
URL	http://www.securityfocus.com/bid/49303/
URL	http://blogs.oracle.com/security/entry/security_alert_for_cve_2011
URL	http://support.apple.com/kb/HT5002
URL	http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html
URL	http://www.oracle.com/technetwork/topics/security/cpujan2012-366304.html
URL	http://www.oracle.com/technetwork/topics/security/alert-cve-2011-3192-485304.html
URL	http://www.gossamer-threads.com/lists/apache/dev/401638
URL	https://issues.apache.org/bugzilla/show_bug.cgi?id=51714
URL	https://www.apache.org/dist/httpd/Announcement2.2.html
URL	https://cwe.mitre.org/data/definitions/399.html

Apache Tomcat End of Life — Low

Solution Details

Upgrade to a supported version of Apache Tomcat.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The version of Apache Tomcat on this host is no longer supported. Vulnerabilities within this version of Apache Tomcat will no longer be fixed by Apache.
Impact:
Even though vulnerabilities in this version of Apache Tomcat may exist, Apache will not patch them. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this host or its data.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	http://tomcat.apache.org/index.html
URL	http://tomcat.apache.org/tomcat-55-eol.html
URL	http://tomcat.apache.org/whichversion.html

Apache Username Disclosure — Low

Vulnerability Details

This host is running the Apache web server with the UserDir feature enabled. It is possible to enumerate users by requesting a URL such as '/~username', a 200 OK or 403 FORBIDDEN response will indicate that account exists on this host, whereas a 404 NOT FOUND or 500 INTERNAL ERROR will indicate the given username is not valid. An attacker can leverage this to gain access to this host.

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

Solution Details

Within the httpd.conf file for this Apache web server, change the 'UserDir public_html' directive to 'UserDir disabled' and restart the web server.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-1013
BUGTRAQ	http://www.securityfocus.com/bid/3335

Debian End of Life — Low

Vulnerability Details

This host is running a version of Debian Linux which is no longer supported. Vulnerabilities associated with this version of Debian cannot be guaranteed to be patched.
Impact:
Unsupported versions of Debian will no longer get updates. Because of this, the OS can be susceptible to vulnerabilities identified in other versions of Debian without any chance of being remediated.

Solution Details

If this asset is required for production, please upgrade the operating system and ensure it is fully patched.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://www.debian.org/releases/
URL	https://endoflife.date/debian

FreeBSD End of Life — Low

Solution Details

Upgrade to a supported version of FreeBSD.

Vulnerability Details

The version of FreeBSD running on this host is no longer supported. Vulnerabilities within this version of FreeBSD will no longer be fixed by the FreeBSD Project.
Impact:
Even though vulnerabilities in this version of FreeBSD may exist, the FreeBSD Project will not patch them. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this host or its data.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://www.freebsd.org/security/unsupported.html

HTTP Host Header Value Reflection — Low

Manual Exploitation

Using the Instance Data in the vulnerability and host information in frontline, you can reproduce the vulnerability as follows.

Example:

Vulnerable asset: 127.0.0.1
Vulnerability found on port: 80

Instance data (portion before the colon is the vulnerable path found. Portion after was the vulnerable match we located)

/bad_page.html : a href="http://vm.frontline.com/new_page.htm>Click here</a>

Based off of this you can manually test it as follows with the vulnerable path being "/bad_page.html".

```
curl -H "Host: vm.frontline.cloud" http://127.0.0.1/bad_page.html
```

"Host: vm.frontline.cloud" is a fake Host header sent with the request and is what to look for returned in the response. Alternatively you can use another hostname such as example.com.

The response received is then searched for the "Host:" url that was sent to see if there are urls in the body of the response that got replaced by it. "a href="http://vm.frontline.com/new_page.htm>Click here</a>" is the link found in the example instance data.

Vulnerability Details

This asset is running a web server service which is hosting an application which reflects the user-supplied Host Header value in the response body. This can lead to XSS and cache poisoning attacks.
Impact:
A remote attacker could leverage this vulnerability to perform XSS, XXE, Cache Poisoning, and other attacks.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Ensure that user-supplied data and header values are not directly used without filtering and validation, especially before being used in a response body.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://www.nginx.com/resources/wiki/start/topics/examples/server_blocks/
URL	https://niiconsulting.com/checkmate/2018/10/manipulating-host-headers-not-anymore/
URL	https://techcommunity.microsoft.com/t5/iis-support-blog/host-header-vulnerability/ba-p/1031958
URL	http://httpd.apache.org/docs/trunk/vhosts/examples.html#defaultallports
URL	https://www.linkedin.com/pulse/host-header-injection-depth-utkarsh-tiwari/

HTTP XML Injection — Low

Solution Details

Ensure that all user supplied input is sanitized for XML escape and control characters. Typical characters which must be sanitized include single quote, double quote, and left and right angle brackets. Please note you should use XML escaping routines to sanitize data instead of manually applying regular expressions to escape individual characters.

Vulnerability Details

This host's web application is vulnerable to an XML injection whereby user supplied input may be inserted and parsed by an XML parser on the web server.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Insecure Crossdomain.xml Directives — Low

Solution Details

Please limit cross-domain access to evaluated and specified sites. See Adobe's recommendations for cross-domain policies at the appropriate link listed in the References List.

Vulnerability Details

This host's URL policy file, crossdomain.xml, allows cross-domain requests from any host. An attacker can leverage this flaw to perform other attacks such as cross-site scripting or cross-site request forgery.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0186
BUGTRAQ	http://www.securityfocus.com/bid/38198
URL	http://www.adobe.com/support/security/bulletins/apsb10-06.html
URL	https://docs.openstack.org/swift/latest/crossdomain.html
URL	http://support.apple.com/kb/HT4188
URL	http://www.adobe.com/support/security/bulletins/apsb10-07.html

Insecure HTML5 Cross Origin Request Policy — Low

Vulnerability Details

This host has one or more pages that contain the Access-Control-Allow-Origin header set to "*", which allows cross-domain requests from any host.
Impact:
An attacker can leverage this flaw to perform other attacks such as cross-site scripting or cross-site request forgery.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please limit cross-domain access to evaluated and specified sites.

Manual Exploitation

This can be tested with the following commands:
Non-SSL:
"curl -I "http://<IP_Address>:<port><path>"
SSL:
"curl -I -k "https://<IP_Address>:<port><path>"

The IP Address is the IP Address of the host. May also be the domain name if thats how the host was scanned.

The Port is the port listed on the right side of the vulnerability trigger.

The Path is listed in the vulnerability trigger details.

You will use the SSL option if underneath the port it has "(SSL)".

If the response has "Access-Control-Allow-Origin: *", this is a legitimate trigger.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://www.owasp.org/index.php/HTML5_Security_Cheat_Sheet
URL	https://cwe.mitre.org/data/definitions/79.html

ISC BIND End Of Life

Low

Solution Details

Update to the latest available supported version.

Vulnerability Details

The version of ISC BIND running on this asset is no longer supported by the vendor.
Impact:
The developers for this software will not release any updates or patches for vulnerabilities that may be discovered in this version of ISC BIND.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://www.isc.org/downloads/software-support-policy/

Microsoft Windows Service Pack Outdated

Low

Solution Details

Please run Windows Update on this host to obtain the latest service pack.

Vulnerability Details

This host does not appear to have the latest supported Microsoft Windows service pack installed. Service pack updates ensure that the system meets some base level of patching and typically contain security enhancements to the base operating system that are not otherwise available as single-security-patches. Vulnerabilities existing on hosts with outdated Windows Service Packs are often much easier to leverage into full system compromises.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://support.microsoft.com/en-us/gp/gp_lifecycle_servicepacksupport
URL	http://support.microsoft.com/sp

MS09-048 Microsoft Windows TCP/IP Remote Code Execution Vulnerabilities

Low

Solution Details

Please apply Microsoft patch MS09-048 to this host. Note: There is no patch for Windows 2000 or Windows XP hosts. According to Microsoft, Windows XP Service Packs 2 and 3 are not affected by these vulnerabilities due to the client firewall not having a listening service. In Windows 2000, the vulnerability is found in the kernel of the operating system, instead of the system libraries. This makes it "infeasible to build the fix for Microsoft Windows 2000 Service Pack 4 to eliminate the vulnerability."

Caveats:
Installing patches can change the functionality and the stability of the host. It is advised that any patches be thoroughly tested and approved before installing on a production system.

Workarounds:
As there is no update for Windows XP or Windows 2000 hosts, ensure firewall best practices are in use. Internet facing hosts should have a minimal number of ports exposed. If possible, enable advanced TCP/IP filtering.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This host is missing Microsoft patch MS09-048. This patch covers three vulnerabilities that affect the

TCP/IP stack in Microsoft Windows.

Certain installations of Microsoft Windows incorrectly process certain packets that have a very small, or zero, window size. Because of this flaw, hosts can become non-responsive or can automatically restart. An attacker can leverage this flaw to cause a denial of service condition.

Next, these installations can improperly clean up state information after processing packets with invalid timestamps. This data can later be referenced by the TCP/IP stack as a function pointer, causing the service to crash. An attacker can leverage this flaw to cause a denial of service, or to cause the service to reference another segment of memory, potentially yielding control of the remote system to the attacker.

Finally, these installations are susceptible to a second denial of service condition. If an application closes a TCP connection with pending data to be sent and an attacker has set a small or zero TCP receive window size, the affected server will not be able to completely close the TCP connection. The attacker can flood the host with these specially crafted packets and cause the affected system to stop responding to new requests.

Impact:
By not applying this patch, this host remains in a vulnerable state. An attacker could force this host to restart repeatedly, or potentially take full control.
Caveats:
This CVC detects the absence of the patch on Windows 2000 and Windows XP Hosts only.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-1925
URL	https://docs.microsoft.com/en-us/security-updates/securitybulletins/2009/ms09-048
URL	https://cwe.mitre.org/data/definitions/94.html

MS22-MAY: Microsoft .NET Security Update — Low

Solution Details

Microsoft has released a fix for this flaw in their May 2022 Security Update. Please download and install the patch from the Microsoft Update Catalog or run Windows Update on the affected asset.

Vulnerability Details

Microsoft has released a security update for Microsoft .NET Framework which includes fixes for the following vulnerabilities:

CVE-2022-30130 - .NET Framework Denial of Service Vulnerability

Affected Products:
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 4.8 on Windows Server 2012 R2
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows Server 2016
Microsoft .NET Framework 3.5 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for 32-bit Systems
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 3.5 on Windows Server 2012
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 3.5 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for x64-based Systems
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for x64-based Systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 20H2 for ARM64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012
Microsoft .NET Framework 4.8 on Windows 10 Version 21H2 for x64-based Systems
Microsoft .NET Framework 4.8 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.6 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 4.8 on Windows Server 2012
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for 32-bit Systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for ARM64-based Systems
Microsoft .NET Framework 3.5 on Windows Server 2012 R2
Microsoft .NET Framework 4.8 on Windows 10 Version 1607 for 32-bit Systems
Microsoft .NET Framework 4.8 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 2.0 Service Pack 2 on Windows Server 2008 for x64-based Systems Service Pack 2
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1809 for x64-based Systems
Microsoft .NET Framework 4.8 on Windows 10 Version 21H1 for 32-bit Systems
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows Server 2019
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016
Microsoft .NET Framework 3.5.1 on Windows 7 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for x64-based Systems
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)

Microsoft .NET Framework 4.8 on Windows 10 Version 21H1 for x64-based Systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 20H2 for x64-based Systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 20H2 for 32-bit Systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2022
Microsoft .NET Framework 3.5.1 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 3.5 AND 4.8 on Windows 11 for ARM64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 10 Version 21H1 for ARM64-based Systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows 11 for x64-based Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows RT 8.1
Microsoft .NET Framework 4.8 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 3.5 on Windows 8.1 for x64-based systems
Microsoft .NET Framework 4.8 on Windows 10 Version 21H2 for ARM64-based Systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2022 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.5 AND 4.8 on Windows 10 Version 1909 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2012 R2 (Server Core installation)
Microsoft .NET Framework 3.5 AND 4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2016 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows RT 8.1
Microsoft .NET Framework 3.5.1 on Windows 7 for 32-bit Systems Service Pack 1
Microsoft .NET Framework 3.0 Service Pack 2 on Windows Server 2008 for 32-bit Systems Service Pack 2
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 8.1 for 32-bit systems
Microsoft .NET Framework 3.5 AND 4.8 on Windows Server 2019 (Server Core installation)
Microsoft .NET Framework 3.5 AND 4.7.2 on Windows 10 Version 1809 for ARM64-based Systems
Microsoft .NET Framework 4.8 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows Server 2008 R2 for x64-based Systems Service Pack 1
Microsoft .NET Framework 4.8 on Windows Server 2012 (Server Core installation)
Microsoft .NET Framework 4.8 on Windows 10 Version 21H2 for 32-bit Systems
Microsoft .NET Framework 4.6/4.6.1/4.6.2/4.7/4.7.1/4.7.2 on Windows 7 for x64-based Systems Service Pack 1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.5

CVSS Vector: AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-30130
URL	https://support.microsoft.com/en-us/help/5013625

Type	Reference
URL	https://support.microsoft.com/en-us/help/5013952
URL	https://support.microsoft.com/en-us/help/5013838
URL	https://support.microsoft.com/en-us/help/5013627
URL	https://support.microsoft.com/en-us/help/5013839
URL	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-30130
URL	https://support.microsoft.com/en-us/help/5013872
URL	https://support.microsoft.com/en-us/help/5013624
URL	https://support.microsoft.com/en-us/help/5013873
URL	https://support.microsoft.com/en-us/help/5013868
URL	https://support.microsoft.com/en-us/help/5013628
URL	https://support.microsoft.com/en-us/help/5013840
URL	https://support.microsoft.com/en-us/help/5013837
URL	https://support.microsoft.com/en-us/help/5013871
URL	https://support.microsoft.com/en-us/help/5013630
URL	https://support.microsoft.com/en-us/help/5013870

NetBIOS Shares With Everyone/Full-Control Permissions — Low

Solution Details

Please remove the 'Everyone' group from the list of users allowed to access this file share.

Vulnerability Details

This host is sharing Windows folders with Full-Control (READ/WRITE) access with the special Windows group of 'EVERYONE'. This Windows group encompasses any user with a valid logon on the domain, no matter how minor their permissions.

Many major computer worms including, Conficker, Stuxnet, and Rorpian utilize shares with 'Everyone' access to write booby-trapped files which spread the infection to other windows hosts which may access these folders.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.4

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0520
URL	http://support.microsoft.com/kb/314984

OpenSSH Local Information Disclosure Vulnerability — Low

Vulnerability Details

authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Please upgrade to the most recent stable release of OpenSSH, available at http://www.openssh.org.

CVSS Base Score: 2.1

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10011
BUGTRAQ	http://www.securityfocus.com/bid/94977
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03818en_us
URL	https://security.netapp.com/advisory/ntap-20171130-0002/
URL	https://www.openssh.com/txt/release-7.4
URL	http://www.slackware.com/security/viewer.php?l=slackware-security&y=2016&m=slackware-security.647637
URL	https://cwe.mitre.org/data/definitions/320.html

Type	Reference
URL	https://github.com/openbsd/src/commit/ac8147a06ed2e2403fb6b9a0c03e618a9333c0e9

OpenSSH scp Client Access Bypass Vulnerability — Low

Solution Details

Please refer to the External References for a link to upgrade to the most recent stable version of OpenSSH.

Vulnerability Details

In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.
Impact:
An attacker can exploit this issue to bypass certain security restrictions and perform unauthorized actions; this may aid in launching further attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.6

CVSS Vector: AV:N/AC:H/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-20685
BUGTRAQ	http://www.securityfocus.com/bid/106531
URL	https://cwe.mitre.org/data/definitions/284.html
URL	https://sintonen.fi/advisories/scp-client-multiple-vulnerabilities.txt
URL	https://github.com/openssh/openssh-portable/commit/6010c0303a422a9c5fa8860c061bf7105eb7f8b2
URL	https://cvsweb.openbsd.org/cgi-bin/cvsweb/src/usr.bin/ssh/scp.c.diff?r1=1.197&r2=1.198&f=h
URL	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2018-20685
URL	https://www.openssh.com/

Type	Reference
URL	https://www.oracle.com/technetwork/security-advisory/cpuapr2019-5072813.html
URL	https://security.netapp.com/advisory/ntap-20190215-0001/

OpenSSH Security Advisory — Low

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf.

Solution Details

Update to the most recent stable version of OpenSSH.

CVSS Base Score: 3.7

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-36368
URL	https://www.openssh.com/security.html
URL	https://www.openssh.com/

OpenSSH 'sshd' Monitor Component Local Impersonation Vulnerability — Low

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

Vulnerability Details

The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 1.9

CVSS Vector: AV:L/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6563
BUGTRAQ	http://www.securityfocus.com/bid/76317
URL	http://www.openssh.com/txt/release-7.0
URL	https://github.com/openssh/openssh-portable/commit/d4697fe9a28dab7255c60433e4dd23cf7fce8a8b
URL	https://security.netapp.com/advisory/ntap-20180201-0002/
URL	https://support.apple.com/HT205375
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2016-2867206.html

OpenSSL AES-NI CBC Padding Oracle Attack — Low

Solution Details

Update to the latest version of OpenSSL.

Vulnerability Details

Older versions of OpenSSL, before 1.0.1t and 1.0.2 before 1.0.2h, do not properly implement AES-NI. During a certain padding check, the vulnerable implementation does not consider memory allocation, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session.
Impact:
An attacker can use this flaw to decrypt some ciphertext, potentially exposing sensitive information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.6

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2107
BUGTRAQ	http://www.securityfocus.com/bid/91787
BUGTRAQ	http://www.securityfocus.com/bid/89760
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html
URL	https://support.apple.com/HT206903
URL	http://support.citrix.com/article/CTX212736
URL	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40202
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03756en_us
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03765en_us
URL	https://security.netapp.com/advisory/ntap-20160504-0001/
URL	http://source.android.com/security/bulletin/2016-07-01.html

Type	Reference
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2018-4428296.html
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10160
URL	http://web-in-security.blogspot.ca/2016/05/curious-padding-oracle-in-openssl-cve.html
URL	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
URL	http://packetstormsecurity.com/files/136912/Slackware-Security-Advisory-openssl-Updates.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05164862
URL	https://blog.cloudflare.com/yet-another-padding-oracle-in-openssl-cbc-ciphersuites/
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03726en_us
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05386804
URL	https://www.tenable.com/security/tns-2016-18
URL	https://git.openssl.org/?p=openssl.git;a=commit;h=68595c0c2886e7942a14f98c17a55a88afb6c292
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05320149
URL	https://bto.bluecoat.com/security-advisory/sa123
URL	https://www.openssl.org/news/secadv/20160503.txt
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03728en_us

OpenSSL End of Life — Low

Solution Details

Upgrade to a supported version of OpenSSL.

Vulnerability Details

The version of OpenSSL running on this host is no longer supported. Vulnerabilities within this version of OpenSSL will no longer be fixed .
Impact:
Even though vulnerabilities in this version of OpenSSL may exist, they will not be patched. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this host or its data.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

PHP End of Life — Low

Solution Details

Upgrade to a currently supported version of PHP.

Vulnerability Details

The installed version of PHP has reached "End-of-Life" status. This means PHP is no longer releasing updates or supporting this version of PHP. Any vulnerabilities present in this version of PHP will not be patched by PHP.
Impact:
Even though vulnerabilities in this version of PHP may exist, PHP will not patch them. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this host or its data.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	http://www.php.net/eol.php

PHP 'ext/standard/info.c' Sensitive Information Disclosure — Low

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

The phpinfo implementation in ext/standard/info.c in PHP before 5.4.30 and 5.5.x before 5.5.14 does not ensure use of the string data type for the PHP_AUTH_PW, PHP_AUTH_TYPE, PHP_AUTH_USER, and PHP_SELF variables, which might allow context-dependent attackers to obtain sensitive information from process memory by using the integer data type with crafted values, related to a "type confusion" vulnerability, as demonstrated by reading a private SSL key in an Apache HTTP Server web-hosting environment with mod_ssl and a PHP 5.3.x mod_php.
Impact:
An attacker could obtain sensitive information from process memory.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.6

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-4721
URL	http://php.net/downloads.php
URL	https://www.sektioneins.de/en/blog/14-07-04-phpinfo-infoleak.html
URL	https://bugs.php.net/bug.php?id=67498
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	https://cwe.mitre.org/data/definitions/200.html

PHP 'gdImageColorMatch' Buffer Overflow Vulnerability — Low

Solution Details

Refer to the External References section for a link to upgrade to the most recent stable version of PHP.

Vulnerability Details

gdImageColorMatch in gd_color_match.c in the GD Graphics Library (aka LibGD) 2.2.5, as used in the imagecolormatch function in PHP before 5.6.40, 7.x before 7.1.26, 7.2.x before 7.2.14, and 7.3.x before 7.3.1, has a heap-based buffer overflow. This can be exploited by an attacker who is able to trigger

imagecolormatch calls with crafted image data.
Impact:
An attacker can exploit these issues to execute arbitrary code in the context of the user running the affected application. Failed exploit attempts will likely result in denial-of-service conditions.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-6977
BUGTRAQ	http://www.securityfocus.com/bid/106731
URL	https://security.netapp.com/advisory/ntap-20190315-0003/
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://bugs.php.net/bug.php?id=77270
URL	http://php.net/ChangeLog-5.php
URL	http://php.net/ChangeLog-7.php
URL	http://php.net/downloads.php
URL	http://packetstormsecurity.com/files/152459/PHP-7.2-imagecolormatch-Out-Of-Band-Heap-Write.html

Phpinfo.php System Information Disclosure — Low

Solution Details

Inside of the php.ini file, change the line that includes the "disable_functions" directive to include "phpinfo".

Example:
disable_functions = phpinfo

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This host is running a third-party web content program. Several third-party web content vendors (including Zend, Invision, and Mambo) include a publicly available script in the web root named 'phpinfo.php'. Any user of the website can view this file, which contains sensitive information about the web server itself, such as environment variables, directory information, and user names. An attacker can leverage this information to help focus his attacks.

CVSS Base Score: 2.6

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

PHP PEAR_REST Arbitrary File Write Vulnerability — Low

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

The PEAR_REST class in REST.php in PEAR in PHP through 5.6.0 allows local users to write to arbitrary files via a symlink attack on a (1) rest.cachefile or (2) rest.cacheid file in /tmp/pear/cache/, related to the retrieveCacheFirst and useLocalCache functions.
Impact:
A local attacker could use this flaw to perform a symbolic link attack against a user (typically the root user) running a pear command (such as "pear install").

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 3.6

CVSS Vector: AV:L/AC:L/Au:N/C:N/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-5459
URL	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=759282
URL	http://php.net/downloads.php
URL	https://cwe.mitre.org/data/definitions/59.html

PHP 'PHP-FPM' Information Disclosure Vulnerability — Low

Vulnerability Details

An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.
Impact:
An attacker could learn valuable information about the target asset that could aid in future attacks.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

CVSS Base Score: 1.9

CVSS Vector: AV:L/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-10545
BUGTRAQ	http://www.securityfocus.com/bid/104022
URL	http://php.net/downloads.php
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://security.netapp.com/advisory/ntap-20180607-0003/
URL	http://php.net/ChangeLog-7.php
URL	https://www.tenable.com/security/tns-2018-12
URL	http://php.net/ChangeLog-5.php
URL	https://bugs.php.net/bug.php?id=75605

PHP '/tmp/phpglibccheck' File Overwrite Vulnerability — Low

Solution Details

Upgrade to the most recent stable version of PHP. Refer to the External References section for more information.

Vulnerability Details

acinclude.m4, as used in the configure script in PHP 5.5.13 and earlier, allows local users to overwrite arbitrary files via a symlink attack on the /tmp/phpglibccheck file.
Impact:
A symlink attack could be launched against the running ./configure script.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 3.3

CVSS Vector: AV:L/AC:M/Au:N/C:N/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3981
URL	http://support.apple.com/kb/HT6443
URL	https://cwe.mitre.org/data/definitions/59.html
URL	https://bugs.php.net/bug.php?id=67390
URL	https://support.apple.com/HT204659
URL	http://git.php.net/?p=php-src.git;a=commit;h=91bcadd85e20e50d3f8c2e9721327681640e6f16
URL	http://php.net/downloads.php
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1104978
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html

Product Has Reached End-of-Life Status — Low

Vulnerability Details

The installed version of this application has reached "End-of-Life" status. This means the vendor is no longer releasing updates or supporting this application. Any vulnerabilities present in the software will not be patched by the vendor.

Solution Details

If this application is necessary for production, please contact the vendor for the most current version of this application. If this application is not necessary, please remove or disable it on this host.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Protocol Allows Authentication Over Clear Text — Low

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Use an encrypted version of this service. The following table provides some examples of services which do authentication over clear text and their encrypted secure counterparts:

ftp -> sftp
telnet -> ssh
imap -> imaps
pop3 -> pop3s

Vulnerability Details

This host is running a service which performs authentication in an insecure manner over clear text.
Impact:
An attacker could utilize a variety of methods to intercept the authentication exchange and gain access to this host.
Caveats:
Depending on the authentication mechanism used, the attacker may not be able to extract the clear text username and/or password.

CVSS Base Score: 3.3

CVSS Vector: AV:A/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Quote Of The Day Service — Low

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Unless it is required, please disable 'qotd'.
This can be done on Unix-based machines by 'commenting out' the qotd entry in the /etc/inetd.conf file by placing a '#' in front of the qotd line and restarting inetd ('killall -HUP inetd').
On Windows machines, click 'Start' - 'Control Panel' and double click 'Administrative Tools' - 'Services'. Scroll down and right-click on 'Simple TCP/IP Services' and select 'Properties'. Under the 'General' tab, change the startup type to 'Manual', then click the 'Stop' button under 'Service Status' and click 'OK'. Note that this will also disable the 'Echo', 'Discard', 'Character Generator', and 'Daytime' service (all of which are unnecessary services).

Vulnerability Details

This host is running the Quote of the Day service. This service provides no functionality other than printing out various quotes. This service can be leveraged to create a DoS condition.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0103
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-233-01
URL	http://www.cert.org/advisories/CA-1996-01.html

Samba End of Life

Low

Vulnerability Details

The installed version of Samba has reached "End-of-Life" status. This means Samba is no longer releasing updates or supporting this version of Samba. Any vulnerabilities present in this version of Samba will not be patched by Samba.
Impact:
Even though vulnerabilities in this version of Samba may exist, Samba will not patch them. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this host or its data.

Solution Details

Upgrade to a currently supported version of Samba.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://wiki.samba.org/index.php/Samba_Release_Planning

Slowloris Resource Depletion And Denial Of Service | Low

Solution Details

This attack can be mitigated by; 1) limiting the number of inactive concurrent web server connections a single user may be allowed to maintain, or 2) setting a minimum threshold of data per second a web server connection is allowed to maintain without being dropped.

Examples of applicable apache modules useful for implementing suggested remediation include:
mod_reqtimeout - http://httpd.apache.org/docs/2.3/mod/mod_reqtimeout.html
mod_qos - http://sourceforge.net/projects/mod-qos/
mod_cband - http://cband.linux.pl
mod_limitpconn - http://dominia.org/djao/limitipconn.html
mod_evasive - http://www.networkdweebs.com/stuff/security.html
mod_security - http://www.modsecurity.org/
mod_antiloris - ftp://ftp.monshouwer.eu/pub/linux/mod_antiloris/

Additional third party modules may also be available. Please contact the vendor for additional information.

Vulnerability Details

This host is running a web server that appears to utilize a configuration which allows a single remote host to consume all connection resources. The slowloris denial of service is achieved by systematically establishing and maintaining connections through partial header requests and http keepalive messages. The attacker can continue this methodology until all web server connections are tied up, resulting in a complete denial of service to legitimate users. Web servers that utilize threading are more susceptible to a slowloris attack. In contrast to other web server denial of service techniques, this attack only requires a tiny amount of bandwidth and a single host IP address.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-6750
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-5568

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/21865
BUGTRAQ	http://www.securityfocus.com/bid/56686
URL	http://threatpost.com/en_us/blogs/mitigating-slowloris-http-dos-attack-062209
URL	http://www.apachelounge.com/viewtopic.php?t=3137
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05111017
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05158380
URL	https://cwe.mitre.org/data/definitions/399.html
URL	https://bugzilla.redhat.com/show_bug.cgi?id=880011
URL	http://captainholly.wordpress.com/2009/06/19/slowloris-vs-tomcat/
URL	https://cwe.mitre.org/data/definitions/16.html

SMB Security Signatures Not Required — Low

Solution Details

In order to remediate this vulnerability, you must require SMB signing on both clients and servers. The most effective way to require SMB signing is by making the following changes to your domain group policy:

Microsoft network client: Digitally sign communications (always) Policy Setting: Enabled

Microsoft network server: Digitally sign communications (always) Policy Setting: Enabled

Please note that this setting may cause issues with third-party applications and devices, such as multi-function copiers/printers and some versions of MacOS, from properly authenticating to your domain if they do not support SMB signing. We recommend placing these types of devices in a separate domain group in which SMB signing is not required.

For a generic overview of SMB signing, please consult the following links:
https://blogs.technet.microsoft.com/josebda/2010/12/01/the-basics-of-smb-signing-covering-both-smb1-and-smb2/
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-always
https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always

For Linux, use the following setting in smb.conf in the [global] section. File typically located at /etc/samba/smb.conf.

```
client signing = mandatory
server signing = mandatory
```

Vulnerability Details

This host does not appear to require SMB Security Signatures when communicating with peers. When SMB signing is required, both computers in the SMB connection must support SMB signing. SMB Security Signatures provide a more secure communication path on Microsoft Windows Domains by ensuring that authenticated session messages cannot be relayed by a man-in-the-middle attacker.

By intercepting challenge/response sequences, a remote unauthenticated attacker may be able obtain session keys which can be used to authenticate to the domain controller with the privileges of the affected user.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 3.2

CVSS Vector: AV:A/AC:H/Au:N/C:P/I:P/A:N

Type	Reference
URL	https://www.stigviewer.com/stig/red_hat_enterprise_linux_6/2013-02-05/finding/RHEL-06-000272
URL	https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
URL	https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing

SMB User Enumeration — Low

Solution Details

If this host does not need to share resources (file/printer sharing, RPC, etc.), disable the Server Service. By disabling the Server Service, the machine can still participate in a domain, but will no longer allow it's resources to be shared on the network (i.e. an attached printer, fixed disks, etc.). If this host is accessible externally, we recommend that access be filtered to TCP ports 135, 138, 139, and 445 as well as UDP ports 137, 138, and 139.

Vulnerability Details

This host is running a Samba server with SMB NULL sessions enabled, which was used to obtain a list of the users on this host. Please see the Data Section for the list of users that was retrieved.
Impact:

SMB NULL sessions allow an attacker to query for the usernames of accounts on this host. Once an attacker has the account names, it may be possible to launch brute force or password guessing attacks.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

SMTP Server EXPN/VRFY — Low

Solution Details

For Sendmail; in /etc/sendmail.cf add the option 'O PrivacyOptions=goaway'.
For other vendors; refer to the application documentation, or contact the vendor for proper settings.

Vulnerability Details

This host is running a SMTP mail server that answers to the EXPN and/or VRFY commands. The EXPN command can be used to find the delivery address of mail aliases, or even the full name of the recipients. The VRFY command may be used to check the validity of an account. An attacker can leverage these commands to gather information about user accounts for use in brute force attacks or social engineering.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

SSH Protocol 1 Enabled — Low

Vulnerability Details

This host accepts Secure Shell (SSH) connections that are encrypted using version 1 of the SSH protocol (SSH-1). Several cryptographic weaknesses are inherent in SSH-1, which make it unsuitable for use in a production environment. These weaknesses include the recovery of a session key as well as susceptibility to the CRC32 Compensation Attack Detector. Exploitation of either of the mentioned

attack vectors can result in complete compromise of the vulnerable server.
Impact:
If a host is running an SSH server that supports SSH-1, users of the system can compromise the security of the system by being subjected to a man-in-the-middle attack. An attacker who is able to eavesdrop on the communication between the client and the server will be able to replay packets, discover the session key, or otherwise submit legitimate requests to the SSH-1 server under the context of the connecting client who is being exploited.

The extent of the impact of this attack will depend on the privileges of the user who is exploited by an attacker.

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

Manual Exploitation

A command of the following form will establish a connection from the localhost to a remote machine on standard command-line SSH tools:

```
ssh -1 <username>@<remotehostname or IP address>
```

```
e.g. ssh -1 jsmith@192.168.0.3
```

That command will attempt to establish a session over SSH-1 with the remote host that has IP address 192.168.0.3 using the username 'jsmith'.

Solution Details

It is recommended that use of SSH-1 be disabled on the vulnerable server.

In OpenSSH implementations, this can be accomplished by modifying the sshd_config file on the server. Change the 'Protocol' option to read 'Protocol 2' and remove any other 'Protocol' option lines from the sshd_config file.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-1473
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-0572
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-0361
BUGTRAQ	http://www.securityfocus.com/bid/2344
URL	https://cwe.mitre.org/data/definitions/310.html
URL	ftp://ftp.ssh.com/pub/ssh/

Type	Reference
URL	http://www.cisco.com/warp/public/707/SSH-multiple-pub.html
URL	http://www.cisco.com/en/US/docs/ios/12_3t/12_3t4/feature/guide/gt_ssh2.html

SSL Connection: RSA Export Grade Cipher FREAK Vulnerability — Low

Solution Details

To fix this vulnerability, disable all SSL export grade ciphers listed in the data section of this vulnerability.

For Apache Servers:
Add the "!EXP" directive to the "SSLCipherSuite" setting in the httpd.conf file.

For IIS Servers:
See KB-Item KB245030 (linked in the references section) and disable all ciphers with "EXPORT" in the name.

Vulnerability Details

This server allows for encrypted connections using RSA Export grade ciphers, allowing Man in the Middle attackers to conduct 'SSL FREAK' (Factoring Attack on RSA-EXPORT Keys) attacks which can result in all encrypted traffic between this server and affected clients to be decrypted in a brute-force fashion.

Because modern web servers often don't generate fresh RSA keys for every single connection, and will often generate them on startup and use them so long as the server remains running, this can cause a single factored RSA key attack carried out against a single client to be reused to affect other current and future connections to the server (until it is restarted).

Recent vulnerability disclosures in SSL implementations indicate that this attack is often available even if the client claims to reject SSL-Export-Grade ciphers which is why it must be disabled on the server to ensure that the confidentiality of encrypted connections is maintained.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0204
BUGTRAQ	http://www.securityfocus.com/bid/71936

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/91787
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21883640
URL	https://github.com/openssl/openssl/commit/ce325c60c74b0fa784f5872404b722e120e5cab0
URL	https://support.apple.com/HT204659
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10679
URL	https://bto.bluecoat.com/security-advisory/sa88
URL	https://www.openssl.org/news/secadv_20150108.txt
URL	http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
URL	http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
URL	http://blog.cryptographyengineering.com/2015/03/attack-of-week-freak-or-factoring-nsa.html
URL	http://support.microsoft.com/kb/245030
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2018-4258247.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinapr2015-2511959.html
URL	http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
URL	https://cwe.mitre.org/data/definitions/310.html
URL	http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	https://support.citrix.com/article/CTX216642
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html

Type	Reference
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21960769
URL	https://bto.bluecoat.com/security-advisory/sa91
URL	https://www.openssl.org/news/secadv_20150319.txt
URL	http://support.novell.com/security/cve/CVE-2015-0204.html

SSL Connection: Server Appears Vulnerable to ChangeCipherSpec Injection

Low

Vulnerability Details

This host is running a web server which is utilizing a version of OpenSSL that appears to be susceptible to a change cipher spec injection vulnerability. This vulnerability is a flaw in the implementation of OpenSSL that may allow an attacker to observe connection content between a client and this server via a man-in-the-middle type of attack.

This vulnerability affects all current SSL protocol versions, including: SSL3.0, TLS1.0, TLS1.1, TLS1.2.

Please be aware that this is an experimental vulnerability check. If the scanner indicates that your server may allow early CCS, you need to still confirm that the target is in fact OpenSSL in the affected range as outlined in the OpenSSL security advisory.
Impact:
An attacker who exploits this vulnerability must utilize a man-in-the-middle attack in order to get any benefit from the vulnerability. As a result of this, the severity of this vulnerability is considered much lower than that of the OpenSSL Heartbleed flaw. This is generally the case when the web server is only accessible via the local network. However, if a server is accessible via the Internet, the severity increases somewhat as there is a greater potential for a man-in-the-middle attack.

Regardless of whether the server is exposed internally or externally, if an attacker is able to obtain a privileged position between a client and this server, it may be possible to read all sensitive data that is passing between the two hosts by abusing this flaw.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

This vulnerability is reported to affect versions of OpenSSL including:

OpenSSL 1.0.1 through 1.0.1g
OpenSSL 1.0.0 through 1.0.0l
all versions before OpenSSL 0.9.8y

Non-affected versions include:

OpenSSL 1.0.1h
OpenSSL 1.0.0m
OpenSSL 0.9.8za

OpenSSL has released updated versions of the library that address this vulnerability. Please upgrade to the latest version.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0224
URL	http://www.oracle.com/technetwork/topics/security/cpuoct2014-1972960.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
URL	http://www.vmware.com/security/advisories/VMSA-2014-0012.html
URL	http://www.oracle.com/technetwork/topics/security/cpujul2014-1972956.html
URL	http://support.apple.com/kb/HT6443
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676786
URL	http://www-01.ibm.com/support/docview.wss?uid=isg400001841
URL	http://www-01.ibm.com/support/docview.wss?uid=isg400001843
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676655
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676501
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676419
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676062
URL	http://www.ibm.com/support/docview.wss?uid=swg24037783
URL	http://www.vmware.com/security/advisories/VMSA-2014-0006.html
URL	https://www.novell.com/support/kb/doc.php?id=7015271

Type	Reference
URL	http://aix.software.ibm.com/aix/efixes/security/openssl_advisory9.asc
URL	http://www-01.ibm.com/support/docview.wss?uid=nas8N1020163
URL	http://www.kerio.com/support/kerio-control/release-history
URL	https://filezilla-project.org/versions.php?type=server
URL	http://www.innominate.com/data/downloads/manuals/mdm_1.5.2.1_Release_Notes.pdf
URL	http://ccsinjection.lepidum.co.jp/
URL	https://www.openssl.org/news/secadv_20140605.txt
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21678167
URL	https://www.imperialviolet.org/2014/06/05/earlyccs.html
URL	https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=bc8923b1ec9c467755cd86f7848c50ee8812e441
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1103586
URL	https://access.redhat.com/site/blogs/766093/posts/908133
URL	http://ccsinjection.lepidum.co.jp
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21678289
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21677390
URL	http://www-01.ibm.com/support/docview.wss?uid=ssg1S1004690
URL	http://www-01.ibm.com/support/docview.wss?uid=nas8N1020172
URL	http://www.splunk.com/view/SP-CAAAM2D
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676833
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21678233
URL	http://puppetlabs.com/security/cve/cve-2014-0224
URL	http://linux.oracle.com/errata/ELSA-2014-1053.html
URL	https://cwe.mitre.org/data/definitions/310.html

Type	Reference
URL	http://support.citrix.com/article/CTX140876
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676529
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21677836
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676644
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21683332
URL	http://www.ibm.com/support/docview.wss?uid=swg21676356
URL	http://www.f-secure.com/en/web/labs_global/fsc-2014-6
URL	http://www-01.ibm.com/support/docview.wss?uid=swg24037870
URL	http://www.ibm.com/support/docview.wss?uid=ssg1S1004678
URL	http://www.ibm.com/support/docview.wss?uid=swg21676877
URL	https://blogs.oracle.com/sunsecurity/entry/cve_2014_0224_cryptographic_issues1
URL	https://www.ibm.com/support/docview.wss?uid=ssg1S1004670
URL	https://www.ibm.com/support/docview.wss?uid=ssg1S1004671
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
URL	http://www.openssl.org/news/secadv_20140605.txt
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10075
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21675626
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21675821
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21676071
URL	http://www.novell.com/support/kb/doc.php?id=7015300
URL	http://www.novell.com/support/kb/doc.php?id=7015264
URL	http://www.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-345106.htm
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21677828

Type	Reference
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21677695
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html

SSL Connection: Server Vulnerable to Bar Mitzvah Attack — Low

Solution Details

Disable support for the RC4 cipher suites in favor of TLS 1.2 AES-GCM cipher suites. Consult your specific vendor documentation for more information.

Vulnerability Details

The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase. This makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values. This is also known as the "Bar Mitzvah" issue.
Impact:
A successful attack against a TLS/SSL session that uses the RC4 cipher could result in a leak of a limited amount of plaintext such as user credentials.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2808
BUGTRAQ	http://www.securityfocus.com/bid/73684
BUGTRAQ	http://www.securityfocus.com/bid/91787
URL	https://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5098709
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21960769

Type	Reference
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05289935
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05336888
URL	http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
URL	https://cwe.mitre.org/data/definitions/310.html
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10163
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21903565
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04779034
URL	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
URL	https://kb.juniper.net/JSA10783
URL	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html
URL	https://www.blackhat.com/docs/asia-15/materials/asia-15-Mantin-Bar-Mitzvah-Attack-Breaking-SSL-With-13-Year-Old-RC4-Weakness-wp.pdf
URL	http://www.huawei.com/en/psirt/security-advisories/hw-454055
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05085988
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05193347
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10727
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04926789

Type	Reference
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04770140
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04772190
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04773119
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04773256
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21960015
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04708650
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04711380
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21883640

SSL Connection: SSLv3 CBC Mode Cipher POODLE Vulnerability — Low

Vulnerability Details

This host is susceptible to the SSL version 3 POODLE (Padding Oracle On Downgraded Legacy Encryption) attack. By using SSL version 3 and CBC Mode ciphers this host can allow an attacker to expose encrypted data in a connection between the client and server.
Impact:
Over time, an attacker can steal sensitive information between the client and the server using this man in the middle attack. Hosts may default to a more secure protocol (TLS 1.2, for example), but a network attacker could potentially trigger a reconnection causing the browser to retry older protocols (SSL version 3).

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

It is recommended that SSL 3.0 be disabled to avoid this and other related vulnerabilities. However, due to backwards compatibility concerns, it may be necessary to leave this protocol enabled. In this case disabling CBC ciphers will also prevent this attack. It is also recommended that the client and server be updated to support the TLS_FALLBACK_SCSV mechanism. This ensures that SSL 3.0 is only used in legacy situations, and prevents attackers from forcing a protocol downgrade.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566
BUGTRAQ	http://www.securityfocus.com/bid/70574
URL	http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-3566.html
URL	http://blog.cryptographyengineering.com/2014/10/attack-of-week-poodle.html
URL	http://askubuntu.com/questions/537196/how-do-i-patch-workaround-sslv3-poodle-vulnerability-cve-2014-3566
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	http://downloads.asterisk.org/pub/security/AST-2014-011.html
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02
URL	https://www.suse.com/support/kb/doc.php?id=7015773
URL	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04779034
URL	https://www.openssl.org/news/secadv_20141015.txt
URL	https://support.apple.com/kb/HT6541
URL	https://support.lenovo.com/us/en/product_security/poodle
URL	https://technet.microsoft.com/library/security/3009008.aspx
URL	https://www.imperialviolet.org/2014/10/14/poodle.html
URL	https://www.openssl.org/~bodo/ssl-poodle.pdf
URL	http://googleonlinesecurity.blogspot.com/2014/10/this-poodle-bites-exploiting-ssl-30.html
URL	https://support.apple.com/kb/HT6542
URL	https://github.com/mpgn/poodle-PoC
URL	https://support.apple.com/kb/HT6531
URL	https://support.apple.com/kb/HT6529

Type	Reference
URL	https://support.apple.com/kb/HT6527
URL	https://bto.bluecoat.com/security-advisory/sa83
URL	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10091
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10090
URL	https://blogs.oracle.com/sunsecurity/entry/multiple_vulnerabilities_in_openssl6
URL	http://support.apple.com/HT204244
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21687172
URL	https://support.citrix.com/article/CTX216642
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2015-2370101.html
URL	https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/
URL	http://www.oracle.com/technetwork/topics/security/bulletinoct2015-2511968.html
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21687611
URL	http://advisories.mageia.org/MGASA-2014-0416.html
URL	http://www-01.ibm.com/support/docview.wss?uid=isg3T1021439
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
URL	https://www.elastic.co/blog/logstash-1-4-3-released
URL	http://www-01.ibm.com/support/docview.wss?uid=isg3T1021431
URL	http://blog.nodejs.org/2014/10/23/node-v0-10-33-stable/
URL	https://groups.google.com/forum/#!topic/docker-user/oYm0i3xShJU

Type	Reference
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21692299
URL	https://access.redhat.com/articles/1232123
URL	https://security.netapp.com/advisory/ntap-20141015-0001/
URL	https://puppet.com/security/cve/poodle-sslv3-vulnerability
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1152789
URL	https://www-01.ibm.com/support/docview.wss?uid=swg21688165
URL	https://support.apple.com/kb/HT6535
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinapr2015-2511959.html
URL	http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2016-2867206.html
URL	https://cwe.mitre.org/data/definitions/310.html
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21688283
URL	https://devcentral.f5.com/articles/cve-2014-3566-removing-sslv3-from-big-ip
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21686997
URL	http://aix.software.ibm.com/aix/efixes/security/openssl_advisory11.asc
URL	https://support.apple.com/HT205217
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05068681
URL	http://docs.ipswitch.com/MOVEit/DMZ82/ReleaseNotes/MOVEitReleaseNotes82.pdf
URL	https://bugzilla.mozilla.org/show_bug.cgi?id=1076983
URL	https://support.lenovo.com/product_security/poodle

Type	Reference
URL	http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-405500.htm
URL	http://www.vmware.com/security/advisories/VMSA-2015-0003.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04819635
URL	http://www.oracle.com/technetwork/topics/security/cpuapr2015-2365600.html
URL	https://www.cloudera.com/documentation/other/security-bulletins/topics/csb_topic_1.html

SSL Connection: SSL Version 3 Enabled — Low

Vulnerability Details

This host appears to support Secure Sockets Layer version 3 (SSLv3). The National Institute of Standards and Technology (NIST) has identified SSLv3 as “no longer being acceptable for protection of data due to inherent weaknesses within the protocol." This is in large part due to the many reported vulnerabilities within various implementations of SSLv3, including high profile vulnerabilities such as Heartbleed and POODLE.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Due to its inherent weaknesses, please consider disabling support for SSLv3 and only supporting Transport Layer Security (TLS) version 1.2. Consult your specific vendor documentation for more information.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	http://en.wikipedia.org/wiki/Transport_Layer_Security

SSL Connection: TLS Diffie-Hellman Export Cipher Downgrade Logjam Vulnerability — Low

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Disable export grade cipher suites, generate a unique 2048-bit or stronger Diffie-Hellman group, and enable Elliptic-Curve Diffie-Hellman (ECDHE) cipher suites. For more specific remediation instructions, refer to the product's documentation or contact the vendor for support.

Vulnerability Details

This server allows encrypted connections using a TLS export grade cipher suite that uses the Diffie-Hellman key exchange algorithm. This allows a man-in-the-middle attacker to conduct the "Logjam" attack on the connection to decrypt the traffic.
Impact:
This server allows encrypted connections using a TLS export grade cipher suite that uses the Diffie-Hellman key exchange algorithm. This allows a man-in-the-middle attacker to conduct the "Logjam" attack on the connection to decrypt the traffic.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-4000
BUGTRAQ	http://www.securityfocus.com/bid/74733
BUGTRAQ	http://www.securityfocus.com/bid/91787
URL	https://www.openssl.org/news/secadv_20150611.txt
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21959325
URL	http://aix.software.ibm.com/aix/efixes/security/sendmail_advisory2.asc
URL	https://developer.mozilla.org/en-US/docs/Mozilla/Projects/NSS/NSS_3.19.1_release_notes
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21960191
URL	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html
URL	https://www-947.ibm.com/support/entry/portal/docdisplay?lndocid=MIGR-5098403
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10681
URL	https://security.netapp.com/advisory/ntap-20150619-0001/

Type	Reference
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21960194
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21960418
URL	https://support.citrix.com/article/CTX216642
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05045763
URL	https://puppet.com/security/cve/CVE-2015-4000
URL	https://help.ecostruxureit.com/display/public/UADCO8x/StruxureWare+Data+Center+Operation+Software+Vulnerability+Fixes
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21959132
URL	http://www.oracle.com/technetwork/topics/security/cpujan2016-2367955.html
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21958984
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21961717
URL	https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbhf03831en_us
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21959812
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21959539
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21959530
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21959517
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21959481
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21959453
URL	https://cwe.mitre.org/data/definitions/310.html
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10122
URL	http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21962739

Type	Reference
URL	http://support.apple.com/kb/HT204942
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21967893
URL	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04876402
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21960041
URL	https://bto.bluecoat.com/security-advisory/sa98
URL	http://h20564.www2.hpe.com/hpsc/doc/public/display?docId=emr_na-c04949778
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05193083
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04953655
URL	http://support.apple.com/kb/HT204941
URL	http://www-304.ibm.com/support/docview.wss?uid=swg21962816
URL	http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
URL	http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10727
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04926789
URL	http://www.oracle.com/technetwork/topics/security/bulletinjan2016-2867206.html
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04770140
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04772190
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04773119
URL	http://www.oracle.com/technetwork/topics/security/bulletinjul2015-2511963.html
URL	https://www.suse.com/security/cve/CVE-2015-4000.html

Type	Reference
URL	http://www.solarwinds.com/documentation/storage/storagemanager/docs/ReleaseNotes/releaseNotes.htm
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04740527
URL	https://openssl.org/news/secadv/20150611.txt
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21959111
URL	http://support.citrix.com/article/CTX201114
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04923929
URL	https://www.openssl.org/blog/blog/2015/05/20/logjam-freak-upcoming-changes/
URL	https://blog.cloudflare.com/logjam-the-latest-tls-vulnerability-explained/
URL	https://bugzilla.mozilla.org/show_bug.cgi?id=1138554
URL	http://www.mozilla.org/security/announce/2015/mfsa2015-70.html
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05128722
URL	https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04918839
URL	https://www-304.ibm.com/support/docview.wss?uid=swg21959745

Ubuntu End of Life — Low

Vulnerability Details

This host is running a version of Ubuntu Linux which is no longer supported. Vulnerabilities associated with this version of Ubuntu cannot be guaranteed to be patched.
Impact:
Unsupported versions of Ubuntu will no longer get updates. Because of this, the OS can be susceptible to vulnerabilities identified in other versions of Ubuntu without any chance of being remediated.

Solution Details

If this host is required for production, please upgrade the operating system and ensure it is fully patched.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://wiki.ubuntu.com/Releases

VMware Security Advisory: VMSA-2018-0027 — Low

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 8.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6982
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-6981
BUGTRAQ	http://www.securityfocus.com/bid/105881
BUGTRAQ	http://www.securityfocus.com/bid/105882
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://www.vmware.com/security/advisories/VMSA-2018-0027.html
URL	https://www.vmware.com/security/advisories/VMSA-2018-0027.html

VMware Security Advisory: VMSA-2019-0005 Low

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.8

CVSS Vector: AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5519
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5518
BUGTRAQ	http://www.securityfocus.com/bid/108443
BUGTRAQ	http://www.securityfocus.com/bid/107535
BUGTRAQ	http://www.securityfocus.com/bid/107541
URL	https://www.vmware.com/security/advisories/VMSA-2019-0005.html
URL	http://packetstormsecurity.com/files/152290/VMware-Security-Advisory-2019-0005.html
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-420/
URL	https://cwe.mitre.org/data/definitions/119.html
URL	https://www.zerodayinitiative.com/advisories/ZDI-19-421/
URL	https://www.vmware.com/security/advisories/VMSA-2019-0005.html

VMware Security Advisory: VMSA-2019-0014 Low

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

CVSS Base Score: 8.8

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5527
URL	https://www.vmware.com/security/advisories/VMSA-2019-0014.html

VMware Security Advisory: VMSA-2019-0019

Low

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 3.5

CVSS Vector: AV:N/AC:M/Au:S/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2019-5536
URL	https://www.vmware.com/security/advisories/VMSA-2019-0019.html

VMware Security Advisory: VMSA-2020-0011

Low

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

This asset is affected by one or more vulnerabilities that could result in denial of service or potentially remote code execution. Please see the vendor advisory, linked in the External References section, for more information.

CVSS Base Score: 5.5

CVSS Vector: AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3958
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-3959
URL	https://www.vmware.com/security/advisories/VMSA-2020-0011.html

VMware Security Advisory: VMSA-2022-0016 Low

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

Vulnerability Details

VMware ESXi contains information leak vulnerabilitieswhenDirectPath I/O (PCI-Passthrough) is utilized. VMware has evaluated the severity of these issues to be in theLow severity rangewith a maximum CVSSv3 base score of3.8.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.7

CVSS Vector: AV:A/AC:M/Au:N/C:C/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-21123,CVE-2022-21125,CVE-2022-21166
URL	https://www.vmware.com/security/advisories/VMSA-2022-0016.html

VMware Security Advisory: VMSA-2022-0020 Low

Vulnerability Details

VMware ESXi containsReturn-Stack-Buffer-Underflow (CVE's-2022-29901, CVE's-2022-28693, CVE's-2022-26373) andBranch Type Confusion(CVE's-2022-23816, CVE's-2022-23825)vulnerabilities due to the Intel and AMD processors it utilizes. VMware has evaluated the severity of these issues to be in theModerate severity rangewith a maximum CVSSv3 base score of5.6.

Solution Details

VMware has released a fix for these flaws which can be downloaded from the VMware update catalog.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:A/AC:M/Au:N/C:N/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2022-29901,CVE-2022-28693,CVE-2022-23816,CVE-2022-23825,CVE-2022-26373
URL	https://www.vmware.com/security/advisories/VMSA-2022-0020.html

VNC Weak Password Encryption — Low

Vulnerability Details

This host is running VNC. VNC contains a security flaw. This version does not support strong encryption of the VNC password which is stored in the registry. This password is encrypted using a static key for an encryption algorithm that is easily crackable in a matter of seconds, and is stored in a registry key that by default has no restrictions on user access. An attacker can leverage this security flaw to retrieve the encrypted password hash and crack it to obtain the VNC password.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Remove this installation of VNC. If remote administration is required, install the Enterprise version of VNC and configure it to use strong encryption and authentication controls or use another product that supports strong encryption and authentication mechanisms.

CVSS Base Score: 3.5

CVSS Vector: AV:L/AC:H/Au:S/C:P/I:P/A:P

Type	Reference
There are no references for this vulnerability.	

Web Server Directory Indexing Enabled

Low

Vulnerability Details

This host's web service has directory indexing enabled, which may expose the location of sensitive files. Attackers can leverage this information to target further attacks.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Disable this feature on production servers.
For Apache, remove the 'Indexes' item from the 'Options' configuration line for the appropriate directory and restart the service.

For IIS, open the Internet Service Manager, right-click the appropriate directory, select Properties, and uncheck the 'Indexes' item.

For other web servers, please refer to the vendor documentation.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0569
URL	https://cwe.mitre.org/data/definitions/200.html

Webserver Expect Header Allows Cross-Site Scripting

Low

Solution Details

Several vendors have provided patches for this flaw.

IBM HTTP Server:
6.0 series: upgrade to version 6.0.2.13 or later
6.1 series: upgrade to version 6.1.0.1 or later

Apache:
2.0 series: upgrade to version 2.0.58 or later
2.2 series: upgrade to version 2.2.2 or later

If neither of these solutions are applicable, please contact the vendor of your web server software for specific remediation instructions.

Vulnerability Details

This host is running a web server that allows reflected cross-site scripting through the Expect HTTP header. An attacker can exploit this flaw by getting the victim's web browser to send a web request to the target web server (this host) with script code in the Expect HTTP header, which will then be reflected back to the victim's web browser and executed. Possible scenarios for this attack include crafted flash files or document files.
Impact:
An attacker that successfully exploits this flaw will be able to run arbitrary script code within the context of the victim's web browser.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:N/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-5944
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-2453
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1543
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2006-3918
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-1700
BUGTRAQ	http://www.securityfocus.com/bid/19661
BUGTRAQ	http://www.securityfocus.com/bid/26457
BUGTRAQ	http://www.securityfocus.com/bid/14473
BUGTRAQ	http://www.securityfocus.com/bid/7344
BUGTRAQ	http://www.securityfocus.com/bid/5011
URL	http://www14.software.ibm.com/webapp/set2/subscriptions/pqvcmjd?mode=18&ID=3117
URL	http://secunia.com/secunia_research/2005-31/advisory/
URL	http://svn.apache.org/viewvc?view=rev&revision=394965

Type	Reference
URL	http://www-1.ibm.com/support/docview.wss?uid=swg24017314
URL	http://www.apache.org
URL	http://www.f-secure.com/en_EMEA/support/security-advisory/fsc-2010-2.html
URL	https://cwe.mitre.org/data/definitions/79.html
URL	http://www.securiteam.com/securitynews/5LP10009FC.html
URL	http://kb.vmware.com/KanisaPlatform/Publishing/466/5915871_f.SAL_Public.html

Web Server Uses Unencrypted/Plaintext Form Password Fields — Low

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Utilize HTTPS for all forms which post sensitive information to the web server.

Vulnerability Details

This host contains a webpage with a security flaw. A form on the webpage is submitting passwords over an insecure protocol such as HTTP rather than HTTPS.
Impact:
An attacker cannot normally leverage this flaw to gain access to the host itself. However, this flaw may be used to intercept authentication credentials passed in plain text which then may be used to access the application.

CVSS Base Score: 2.6

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Type	Reference
URL	https://cwe.mitre.org/data/definitions/522.html

WordPress Unsupported Version — Low

Solution Details

Update to the latest stable version of WordPress.

Vulnerability Details

This asset appears to be hosting a version of WordPress which is no longer supported.
Impact:
Even though vulnerabilities in this version of WordPress may exist, they will likely not be patched. Should any vulnerabilities exist, an attacker might be able to leverage them to gain unauthorized access to this host or its data.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:A/AC:M/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://codex.wordpress.org/WordPress_Versions

Apache ETags Inode Number Disclosure

Trivial

Vulnerability Details

This instance of Apache HTTP Server discloses file inode numbers via the ETag header, and child process IDs (PID) via multipart MIME boundaries.
Impact:
A remote attacker could utilize this information disclosure to focus future attacks.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Apply the ETags directive excluding the Inodes field to your apache.conf, as below

```
<Directory />
...
...
FileETag
...
</Directory>
```

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1418

Type	Reference
BUGTRAQ	http://www.securityfocus.com/bid/6943
BUGTRAQ	http://www.securityfocus.com/bid/6939
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html

Apache HTTP Server Denial of Service — Trivial

Solution Details

Please refer to the External References section for links to supplemental vulnerability information and remediation details.

False Positive Notes

This item is a heuristic check and may be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.

CVSS Base Score: 5.9

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2018-1302
BUGTRAQ	http://www.securityfocus.com/bid/103528
URL	https://security.netapp.com/advisory/ntap-20180601-0004/
URL	https://httpd.apache.org/security/vulnerabilities_24.html
URL	https://cwe.mitre.org/data/definitions/476.html

Apache Server Header Information Disclosure — Trivial

Vulnerability Details

This instance of the Apache web server is configured to disclose version information in the "Server" HTTP header.
Impact:
This configuration could aid an attacker in targeting attacks against this asset.

Solution Details

Apply the 'Prod' modifier to the ServerTokens directive in the apache2.conf file.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://httpd.apache.org/docs/current/mod/core.html#servertokens

Chargen Service Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Disable the Chargen Service on this host.
For Unix systems, edit the /etc/inetd.conf file to comment out the chargen service to prevent this service from running in the future. After making the necessary configurations, please restart inetd.

For Windows systems, the chargen service may be disabled by removing the 'Simple TCP/IP' services from the network configuration.

For Cisco devices, access the enable console. Once in configuration mode, input 'no service tcp-small-servers' and 'no service udp-small-servers' to disable the chargen service.

For other systems, please consult the vendor or the system documentation.

Vulnerability Details

This host is running the character generator service, which is typically only used for testing purposes. Attackers can leverage this service to create a DoS condition on this host.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0103
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-233-01
URL	http://www.cert.org/advisories/CA-1996-01.html

CIS Benchmark Profile — Trivial

Vulnerability Details

The data section indicates which CIS benchmark profile was used during the scan to assist in generating accurate CIS reports in Frontline.

Note, the scanner uses a superset of the checks during the scan so that different levels of reports can be generated using the same scan information.

Solution Details

Not applicable as this is not a vulnerability.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Access this computer from the network' — Trivial

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access this computer from the network>

Impact: If you remove the Access this computer from the network user right on domain controllers for all users, no one will be able to log on to the domain or use network resources. If you remove this user right on member servers, users will not be able to connect to those servers through the network. Successful negotiation of IPsec connections requires that the initiating machine has this right, therefore it is recommended that it is assigned to the Users group. If you have installed optional components such as ASP.NET or Internet Information Services (IIS), you may need to assign this user right to additional accounts that are required by those components. It is important to verify that authorized users are assigned this user right for the computers they need to access the network.

Vulnerability Details

This policy setting allows other users on the network to connect to the computer and is required by various network protocols that include Server Message Block (SMB)based protocols, NetBIOS, Common Internet File System (CIFS), and Component Object Model Plus (COM+). Level 1 - Domain Controller. The recommended state for this setting is: Administrators, Authenticated Users, ENTERPRISE DOMAIN CONTROLLERS. Level 1 - Member Server. The recommended state for this setting is: Administrators, Authenticated Users.

Rationale: Users who can connect from their computer to the network can access resources on target computers for which they have permission. For example, the Access this computer from the network user right is required for users to connect to shared printers and folders. If this user right is assigned to the Everyone group, then anyone in the group will be able to read the files in those shared folders. However, this situation is unlikely for new installations of Windows Server 2003 with Service Pack 1 (SP1), because the default share and NTFS permissions in Windows Server 2003 do not include the Everyone group. This vulnerability may have a higher level of risk for computers that you upgrade from Windows NT 4.0 or Windows 2000, because the default permissions for these operating systems are not as restrictive as the default permissions in Windows Server 2003.

CCE Reference Number: CCE-35818-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Accounts: Rename administrator account' | Trivial

Vulnerability Details

The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console).

Rationale: The Administrator account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

CCE Reference Number: CCE-38233-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.1.5

Solution Details

To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account Impact: You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Accounts: Rename administrator account' Trivial

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename administrator account>

Impact: You will have to inform users who are authorized to use this account of the new account name. (The guidance for this setting assumes that the Administrator account was not disabled, which was recommended earlier in this chapter.)

Vulnerability Details

The built-in local administrator account is a well-known account name that attackers will target. It is recommended to choose another name for this account, and to avoid names that denote administrative or elevated access accounts. Be sure to also change the default description for the local administrator (through the Computer Management console). On Domain Controllers, since they do not have their own local accounts, this rule refers to the built-in Administrator account that was established when the domain was first created.

Rationale: The Administrator account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account, it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination. The built-in Administrator account cannot be locked out, regardless of how many times an attacker might use a bad password. This capability makes the Administrator account a popular target for brute force attacks that attempt to guess passwords. The value of this countermeasure is lessened because this account has a well-known SID, and there are third-party tools that allow authentication by using the SID rather than the account name. Therefore, even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

CCE Reference Number: CCE-38233-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.1.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Accounts: Rename guest account'

Trivial

Solution Details

To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account Impact: There should be little impact, because the Guest account is disabled by default.

Vulnerability Details

The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security.

Rationale: The Guest account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account. it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

CCE Reference Number: CCE-38027-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.1.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Accounts: Rename guest account' Trivial

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Rename guest account>

Impact: There should be little impact, because the Guest account is disabled by default.

Vulnerability Details

The built-in local guest account is another well-known name to attackers. It is recommended to rename this account to something that does not indicate its purpose. Even if you disable this account, which is recommended, ensure that you rename it for added security. On Domain Controllers, since they do not have their own local accounts, this rule refers to the built-in Guest account that was established when the domain was first created.

Rationale: The Guest account exists on all computers that run the Windows 2000 or later operating systems. If you rename this account. it is slightly more difficult for unauthorized persons to guess this privileged user name and password combination.

CCE Reference Number: CCE-38027-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.1.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Allow log on locally' Trivial

Vulnerability Details

This policy setting determines which users can interactively log on to computers in your environment. Logons that are initiated by pressing the CTRL+ALT+DEL key sequence on the client computer keyboard require this user right. Users who attempt to log on through Terminal Services or IIS also require this user right. The Guest account is assigned this user right by default. Although this account is disabled by default, it is recommended that you enable this setting through Group Policy. However, this user right should generally be restricted to the Administrators and Users groups. Assign this user right to the Backup Operators group if your organization requires that they have this capability. Level 1 - Domain Controller. The recommended state for this setting is: Administrators, ENTERPRISE DOMAIN CONTROLLERS. Level 1 - Member Server. The recommended state for this setting is: Administrators.

Rationale: Any account with the Allow log on locally user right can log on at the console of the computer. If you do not restrict this user right to legitimate users who need to be able to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

CCE Reference Number: CCE-37659-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on locally>

Impact: If you remove these default groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected by any changes that you make to the Allow log on locally user rights assignments.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Allow log on through Remote Desktop Services' Trivial

Vulnerability Details

This policy setting determines which users or groups have the right to log on as a Terminal Services client. Remote desktop users require this user right. If your organization uses Remote Assistance as part of its help desk strategy, create a group and assign it this user right through Group Policy. If the help desk in your organization does not use Remote Assistance, assign this user right only to the Administrators group or use the restricted groups feature to ensure that no user accounts are part of the Remote Desktop Users group. Restrict this user right to the Administrators group, and possibly the Remote Desktop Users group, to prevent unwanted users from gaining access to computers on your network by means of the Remote Assistance feature. Level 1 - Domain Controller. The recommended state for this setting is: Administrators. Level 1 - Member Server. The recommended state for this setting is: Administrators, Remote Desktop Users.

Note: A Member Server that holds the Remote Desktop Services Role with Remote Desktop Connection Broker Role Service will require a special exception to this recommendation, to allow the Authenticated Users group to be granted this user right. Note #2: The above lists are to be treated as whitelists, which implies that the above principals need not be present for assessment of this recommendation to pass.

Rationale: Any account with the Allow log on through Terminal Services user right can log on to the remote console of the computer. If you do not restrict this user right to legitimate users who need to log on to the console of the computer, unauthorized users could download and run malicious software to elevate their privileges.

CCE Reference Number: CCE-37072-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.7

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Allow log on through Remote Desktop Services>

Impact: Removal of the Allow log on through Terminal Services user right from other groups or membership changes in these default groups could limit the abilities of users who perform specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Create symbolic links' Trivial

Solution Details

To implement the recommended configuration state, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create symbolic links Impact: In most cases there will be no impact because this is the default configuration, however, on Windows Servers with the Hyper-V server role installed this user right should also be granted to the special group "Virtual Machines" otherwise you will not be able to create new virtual machines.

Vulnerability Details

This policy setting determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object, which can be a file, folder, shortcut or another symbolic link. The difference between a shortcut and a symbolic link is that a shortcut only works from within the Windows shell. To other programs and applications, shortcuts are just another file, whereas with symbolic links, the concept of a shortcut is implemented as a feature of the NTFS file system. Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. For this reason, the privilege for creating symbolic links should only be assigned to trusted users. By default, only Administrators can create symbolic links. Level 1 - Domain Controller. The recommended state for this setting is: Administrators. Level 1 - Member Server. The recommended state for this setting is: Administrators and (when the Hyper-V Role is installed) NT VIRTUAL MACHINE\Virtual Machines.

Rationale: Users who have the Create Symbolic Links user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a Denial of Service attack.

CCE Reference Number: CCE-35823-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.15

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Create symbolic links' Trivial

Vulnerability Details

This policy setting determines which users can create symbolic links. In Windows Vista, existing NTFS file system objects, such as files and folders, can be accessed by referring to a new kind of file system object called a symbolic link. A symbolic link is a pointer (much like a shortcut or .lnk file) to another file system object, which can be a file, folder, shortcut or another symbolic link. The difference between a shortcut and a symbolic link is that a shortcut only works from within the Windows shell. To other programs and applications, shortcuts are just another file, whereas with symbolic links, the concept of a shortcut is implemented as a feature of the NTFS file system. Symbolic links can potentially expose security vulnerabilities in applications that are not designed to use them. For this reason, the privilege for creating symbolic links should only be assigned to trusted users. By default, only Administrators can create symbolic links. Level 1 - Domain Controller. The recommended state for this setting is: Administrators. Level 1 - Member Server. The recommended state for this setting is: Administrators and (when the Hyper-V Role is installed) NT VIRTUAL MACHINE\Virtual Machines.

Rationale: Users who have the Create Symbolic Links user right could inadvertently or maliciously expose your system to symbolic link attacks. Symbolic link attacks can be used to change the permissions on a file, to corrupt data, to destroy data, or as a Denial of Service attack.

CCE Reference Number: CCE-35823-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.15

Solution Details

To implement the recommended configuration state, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create symbolic links>

Impact: In most cases there will be no impact because this is the default configuration, however, on Windows Servers with the Hyper-V server role installed this user right should also be granted to the special group "Virtual Machines" otherwise you will not be able to create new virtual machines.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Deny access to this computer from the network' — Trivial

Vulnerability Details

This policy setting prohibits users from connecting to a computer from across the network, which would allow users to access and potentially modify data remotely. In high security environments, there should be no need for remote users to access data on a computer. Instead, file sharing should be accomplished through the use of network servers. Level 1 - Domain Controller. The recommended state for this setting is to include: Guests, Local account. Level 1 - Member Server. The recommended state for this setting is to include: Guests, Local account and member of Administrators group.

Caution: Configuring a standalone (non-domain-joined) server as described above may result in an inability to remotely administer the server.

Note: Configuring a member server or standalone server as described above may adversely affect applications that create a local service account and place it in the Administrators group - in which case you must either convert the application to use a domain-hosted service account, or remove Local account and member of Administrators group from this User Right Assignment. Using a domain-hosted service account is strongly preferred over making an exception to this rule, where possible.

Rationale: Users who can log on to the computer over the network can enumerate lists of account names, group names, and shared resources. Users with permission to access shared folders and files can connect over the network and possibly view or modify data.

CCE Reference Number: CCE-37954-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.17

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny access to this computer from the network>

Impact: If you configure the Deny access to this computer from the network user right for other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should verify that delegated tasks will not be negatively affected.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Enable computer and user accounts to be trusted for delegation' — Trivial

Vulnerability Details

This policy setting allows users to change the Trusted for Delegation setting on a computer object in Active Directory. Abuse of this privilege could allow unauthorized users to impersonate other users on the network. Level 1 - Domain Controller. The recommended state for this setting is: Administrators. Level 1 - Member Server. The recommended state for this setting is: No One.

Rationale: Misuse of the Enable computer and user accounts to be trusted for delegation user right could allow unauthorized users to impersonate other users on the network. An attacker could exploit this privilege to gain access to network resources and make it difficult to determine what has happened after a security incident.

CCE Reference Number: CCE-36860-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.22

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable computer and user accounts to be trusted for delegation>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Impersonate a client after authentication' Trivial

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Impersonate a client after authentication>

Impact: In most cases this configuration will have no impact. If you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to also assign the user right to IIS_IUSRS.

Vulnerability Details

The policy setting allows programs that run on behalf of a user to impersonate that user (or another specified account) so that they can act on behalf of the user. If this user right is required for this kind of impersonation, an unauthorized user will not be able to convince a client to connect for example, by remote procedure call (RPC) or named pipes to a service that they have created to impersonate that client, which could elevate the unauthorized user's permissions to administrative or system levels. Services that are started by the Service Control Manager have the built-in Service group added by default to their access tokens. COM servers that are started by the COM infrastructure and configured to run under a specific account also have the Service group added to their access tokens. As a result, these processes are assigned this user right when they are started. Also, a user can impersonate an access token if any of the following conditions exist: - The access token that is being impersonated is for this user. - The user, in this logon session, logged on to the network with explicit credentials to create the access token. - The requested level is less than Impersonate, such as Anonymous or Identify. An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client. Level 1 - Domain Controller. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE. Level 1 - Member Server. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE and (when the Web Server (IIS) Role with Web Services Role Service is installed) IIS_IUSRS. Note: A Member Server with Microsoft SQL Server and its optional "Integration Services" component installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale: An attacker with the Impersonate a client after authentication user right could create a service, trick a client to make them connect to the service, and then impersonate that client to elevate the attacker's level of access to that of the client.

CCE Reference Number: CCE-37106-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.25

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Interactive logon: Message text for users attempting to log on' — Trivial

Solution Details

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message text for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.

Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.

Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting specifies a text message that displays to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale: Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons#x2014;for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

CCE Reference Number: CCE-37226-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.7.4

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Interactive logon: Message text for users attempting to log on'

Trivial

Solution Details

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message text for users attempting to log on>

Impact: Users will have to acknowledge a dialog box containing the configured text before they can log on to the computer.

Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers.

Vulnerability Details

This policy setting specifies a text message that displays to users when they log on. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale: Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process. This text is often used for legal reasons for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

Note: Any warning that you display should first be approved by your organization's legal and human resources representatives.

CCE Reference Number: CCE-37226-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.7.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Interactive logon: Message title for users attempting to log on' | Trivial

Solution Details

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message title for users attempting to log on Impact: Users will see a message in a dialog box before they can log on to the server console.

Note: Windows Vista and Windows XP Professional support logon banners that can exceed 512 characters in length and that can also contain carriage-return line-feed sequences. However, Windows 2000-based clients cannot interpret and display these messages. You must use a Windows 2000-based computer to create a logon message policy that applies to Windows 2000-based computers. If you inadvertently create a logon message policy on a Windows Vista-based or Windows XP Professional-based computer and you discover that it does not display properly on Windows 2000-based computers, do the following: Change the setting to Not Defined, and then change the setting to the desired value by using a Windows 2000-based computer.

Important: If you do not reconfigure this setting to Not Defined before reconfiguring the setting using a Windows 2000-based computer, the changes will not take effect properly.

Vulnerability Details

This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale: Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

CCE Reference Number: CCE-37512-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.7.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Interactive logon: Message title for users attempting to log on'

Trivial

Vulnerability Details

This policy setting specifies the text displayed in the title bar of the window that users see when they log on to the system. Configure this setting in a manner that is consistent with the security and operational requirements of your organization.

Rationale: Displaying a warning message before logon may help prevent an attack by warning the attacker about the consequences of their misconduct before it happens. It may also help to reinforce corporate policy by notifying employees of the appropriate policy during the logon process.

CCE Reference Number: CCE-37512-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.7.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, configure the following UI path to a value that is consistent with the security and operational requirements of your organization:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Message title for users attempting to log on>

Impact: Users will have to acknowledge a dialog box with the configured title before they can log on to the computer.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Manage auditing and security log' — Trivial

Vulnerability Details

This policy setting determines which users can change the auditing options for files and directories and clear the Security log. For environments running Microsoft Exchange Server, the Exchange Servers group must possess this privilege on Domain Controllers to properly function. Given this, DCs granting the Exchange Servers group this privilege do conform with this benchmark. If the environment does not use Microsoft Exchange Server, then this privilege should be limited to only Administrators on DCs. Level 1 - Domain Controller. The recommended state for this setting is: Administrators and (when Exchange is running in the environment) Exchange Servers. Level 1 - Member Server. The recommended state for this setting is: Administrators.

Rationale: The ability to manage the Security event log is a powerful user right and it should be closely guarded. Anyone with this user right can clear the Security log to erase important evidence of unauthorized activity.

CCE Reference Number: CCE-35906-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.30

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, configure the following UI path: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log Impact: None. This is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Manage auditing and security log' Trivial

Vulnerability Details

This policy setting determines which users can change the auditing options for files and directories and clear the Security log. For environments running Microsoft Exchange Server, the Exchange Servers group must possess this privilege on Domain Controllers to properly function. Given this, DCs granting the Exchange Servers group this privilege do conform with this benchmark. If the environment does not use Microsoft Exchange Server, then this privilege should be limited to only Administrators on DCs. Level 1 - Domain Controller. The recommended state for this setting is: Administrators and (when Exchange is running in the environment) Exchange Servers. Level 1 - Member Server. The recommended state for this setting is: Administrators.

Rationale: The ability to manage the Security event log is a powerful user right and it should be closely guarded. Anyone with this user right can clear the Security log to erase important evidence of unauthorized activity.

CCE Reference Number: CCE-35906-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.30

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Network access: Named Pipes that can be accessed anonymously' Trivial

Solution Details

To establish the recommended configuration via GP, configure the following UI path:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Named Pipes that can be accessed anonymously>

Impact: Null session access over null session access over named pipes will be disabled unless they are included, and applications that rely on this feature or on unauthenticated access to named pipes will no longer function. The BROWSER named pipe may need to be added to this list if the Computer Browser service is needed for supporting legacy components. The Computer Browser service is disabled by default.

Vulnerability Details

This policy setting determines which communication sessions, or pipes, will have attributes and permissions that allow anonymous access. The recommended state for this setting is: Level 1 - Domain Controller. The recommended state for this setting is: LSARPC, NETLOGON, SAMR and (when the legacy Computer Browser service is enabled) BROWSER. Level 1 - Member Server. The recommended state for this setting is: <blank> (i.e. None), or (when the legacy Computer Browser service is enabled) BROWSER.

Note: A Member Server that holds the Remote Desktop Services Role with Remote Desktop Licensing Role Service will require a special exception to this recommendation, to allow the HydraLSPipe and TermServLicensing Named Pipes to be accessed anonymously.

Rationale: Limiting named pipes that can be accessed anonymously will reduce the attack surface of the system.

CCE Reference Number: CCE-38258-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Network access: Remotely accessible registry paths' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths>

Impact: None - this is the default configuration. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If you want to allow remote access, you must also enable the Remote Registry service.

Vulnerability Details

This policy setting determines which registry paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the winreg registry key. Note: This setting does not exist in Windows XP. There was a setting with that name in Windows XP, but it is called "Network access: Remotely accessible registry paths and sub-paths" in Windows Server 2003, Windows Vista, and Windows Server 2008. Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. The recommended state for this setting is: System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server Applications Software\Microsoft\Windows NT\CurrentVersion

Rationale: The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker could use this information to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

CCE Reference Number: CCE-37194-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Configure 'Network access: Remotely accessible registry paths and sub-paths'

Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to: System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths When a server holds the Active Directory Certificate Services Role with Certification Authority Role Service, the above list should also include: System\CurrentControlSet\Services\CertSvc. When a server has the WINS Server Feature installed, the above list should also include: System\CurrentControlSet\Services\WINS>

Impact: None - this is the default configuration. However, if you remove the default registry paths from the list of accessible ones, remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server could fail, as they require remote access to the registry to properly monitor and manage computers.

Note: If you want to allow remote access, you must also enable the Remote Registry service.

Vulnerability Details

This policy setting determines which registry paths and sub-paths will be accessible over the network, regardless of the users or groups listed in the access control list (ACL) of the winreg registry key.

Note: In Windows XP this setting is called "Network access: Remotely accessible registry paths," the setting with that same name in Windows Vista, Windows Server 2008, and Windows Server 2003 does not exist in Windows XP.

Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value.

The recommended state for this setting is: System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal

Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration
Software\Microsoft\Windows NT\CurrentVersion\Perflib
System\CurrentControlSet\Services\SysmonLog

The recommended state for servers that hold the Active Directory Certificate Services Role with Certification Authority Role Service includes the above list and:
System\CurrentControlSet\Services\CertSvc

The recommended state for servers that have the WINS Server Feature installed includes the above list and: System\CurrentControlSet\Services\WINS

Rationale: The registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack.

CCE Reference Number: CCE-36347-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Disable IPv6 (Ensure TCPIP6 Parameter 'DisabledComponents' is set to '0xff (255)') — Trivial

Solution Details

To establish the recommended configuration, set the following Registry value to 0xff (255) (DWORD):
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:DisabledComponents

Note: This change does not take effect until the computer has been restarted.

Note #2: Although Microsoft does not provide an ADMX template to configure this registry value, a custom .ADM template (Disable-IPv6-Components-KB929852.adm) is provided in the CIS Benchmark Remediation Kit to facilitate its configuration. Be aware though that simply turning off the group policy setting in the .ADM template will not "undo" the change once applied. Instead, the opposite setting must be applied to change the registry value to the opposite state.

Impact: Connectivity to other systems using IPv6 will no longer operate, and software that depends on

IPv6 will cease to function. Examples of Microsoft applications that may use IPv6 include: Remote Assistance, HomeGroup, DirectAccess, Windows Mail. This registry change is documented in Microsoft Knowledge Base article 929852: How to disable IPv6 or its components in Windows.

Note: This registry change does not take effect until the next reboot.

Vulnerability Details

Internet Protocol version 6 (IPv6) is a set of protocols that computers use to exchange information over the Internet and over home and business networks. IPv6 allows for many more IP addresses to be assigned than IPv4 did. Older networking, hosts and operating systems may not support IPv6 natively. The recommended state for this setting is: DisabledComponents - 0xff (255)

Rationale: Since the vast majority of private corporate networks have no need to utilize IPv6 (because they have access to private IPv4 addressing), disabling IPv6 components reduces a possible attack surface that is also harder to monitor the traffic on. As a result, we recommend configuring IPv6 to a Disabled state when it is not needed. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.19.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'

Trivial

Vulnerability Details

This security setting is used by Credential Manager during Backup and Restore. No accounts should have this user right, as it is only assigned to Winlogon. Users' saved credentials might be compromised if this user right is assigned to other entities. The recommended state for this setting is: No One.

Rationale: If an account is given this right the user of the account may create an application that calls into Credential Manager and is returned the credentials for another user.

CCE Reference Number: CCE-37056-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller Impact: None, this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Access Credential Manager as a trusted caller' is set to 'No One'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Access Credential Manager as a trusted caller>

Impact: None - this is the default configuration.

Vulnerability Details

This security setting is used by Credential Manager during Backup and Restore. No accounts should have this user right, as it is only assigned to Winlogon. Users' saved credentials might be compromised if this user right is assigned to other entities. The recommended state for this setting is: No One.

Rationale: If an account is given this right the user of the account may create an application that calls into Credential Manager and is returned the credentials for another user.

CCE Reference Number: CCE-37056-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)'

Trivial

Vulnerability Details

This policy setting determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked out account will remain unavailable. If the value for this policy setting is configured to 0, locked out accounts will remain locked out until an administrator manually unlocks them. Although it might seem like a good idea to configure the value for this policy setting to a high value, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts locked by mistake. Users should be aware of the length of time a lock remains in place, so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer. The recommended state for this setting is: 15 or more minute(s).

Rationale: A denial of service (DoS) condition can be created if an attacker abuses the Account lockout threshold and repeatedly attempts to log on with a specific account. Once you configure the Account lockout threshold setting, the account will be locked out after the specified number of failed attempts. If you configure the Account lockout duration setting to 0, then the account will remain locked out until an administrator unlocks it manually.

CCE Reference Number: CCE-37034-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 1.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to 15 or more minute(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration Impact: Although it may seem like a good idea to configure this policy setting to never automatically unlock an account, such a configuration can increase the number of requests that your organization's help desk receives to unlock accounts that were locked by mistake.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Account lockout duration' is set to '15 or more minute(s)'

Trivial

Vulnerability Details

This policy setting determines the length of time that must pass before a locked account is unlocked and a user can try to log on again. The setting does this by specifying the number of minutes a locked out account will remain unavailable. If the value for this policy setting is configured to 0, locked out accounts will remain locked out until an administrator manually unlocks them. Although it might seem like a good idea to configure the value for this policy setting to a high value, such a configuration will likely increase the number of calls that the help desk receives to unlock accounts locked by mistake. Users should be aware of the length of time a lock remains in place, so that they realize they only need to call the help desk if they have an extremely urgent need to regain access to their computer. The recommended state for this setting is: 15 or more minute(s).

Rationale: A denial of service (DoS) condition can be created if an attacker abuses the Account lockout threshold and repeatedly attempts to log on with a specific account. Once you configure the Account lockout threshold setting, the account will be locked out after the specified number of failed attempts. If you configure the Account lockout duration setting to 0, then the account will remain locked out until an administrator unlocks it manually.

CCE Reference Number: CCE-37034-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 1.2.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to 15 or more minute(s):

<Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout duration>

Impact: Although it may seem like a good idea to configure this policy setting to never automatically unlock an account, such a configuration can increase the number of requests that your organization's help desk receives to unlock accounts that were locked by mistake.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid login attempt(s), but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold Impact: If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting may generate additional help desk calls. If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account Lockout Duration to a relatively low value. If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

Vulnerability Details

This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform with the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 10 or fewer invalid logon attempt(s), but not 0.

Rationale: Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

CCE Reference Number: CCE-36008-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 1.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Account lockout threshold' is set to '10 or fewer invalid logon attempt(s), but not 0' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 10 or fewer invalid login attempt(s), but not 0:

<Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Account lockout threshold>

Impact: If this policy setting is enabled, a locked-out account will not be usable until it is reset by an administrator or until the account lockout duration expires. This setting may generate additional help desk calls. If you enforce this setting an attacker could cause a denial of service condition by deliberately generating failed logons for multiple user, therefore you should also configure the Account

Lockout Duration to a relatively low value. If you configure the Account Lockout Threshold to 0, there is a possibility that an attacker's attempt to discover passwords with a brute force password attack might go undetected if a robust audit mechanism is not in place.

Vulnerability Details

This policy setting determines the number of failed logon attempts before the account is locked. Setting this policy to 0 does not conform with the benchmark as doing so disables the account lockout threshold. The recommended state for this setting is: 10 or fewer invalid logon attempt(s), but not 0.

Rationale: Setting an account lockout threshold reduces the likelihood that an online password brute force attack will be successful. Setting the account lockout threshold too low introduces risk of increased accidental lockouts and/or a malicious actor intentionally locking out accounts.

CCE Reference Number: CCE-36008-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 1.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' — Trivial

Vulnerability Details

This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings. The recommended state for this setting is: Disabled.

Rationale: In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

CCE Reference Number: CCE-37953-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.1.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status Impact: Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the domain controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in safe mode to fix the problem that broke the secure channel. If the current Administrator password does not meet the password requirements, you will not be able to re-enable the Administrator account after it is disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Accounts: Administrator account status' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Administrator account status>

Impact: Maintenance issues can arise under certain circumstances if you disable the Administrator account. For example, if the secure channel between a member computer and the domain controller fails in a domain environment for any reason and there is no other local Administrator account, you must restart in safe mode to fix the problem that broke the secure channel. If the current Administrator password does not meet the password requirements, you will not be able to re-enable the Administrator account after it is disabled. If this situation occurs, another member of the Administrators group must set the password on the Administrator account with the Local Users and Groups tool.

Vulnerability Details

This policy setting enables or disables the Administrator account during normal operation. When a computer is booted into safe mode, the Administrator account is always enabled, regardless of how this setting is configured. Note that this setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings. The recommended state for this setting is: Disabled.

Rationale: In some organizations, it can be a daunting management challenge to maintain a regular schedule for periodic password changes for local accounts. Therefore, you may want to disable the built-in Administrator account instead of relying on regular password changes to protect it from attack. Another reason to disable this built-in account is that it cannot be locked out no matter how many failed logons it accrues, which makes it a prime target for brute force attacks that attempt to guess passwords. Also, this account has a well-known security identifier (SID) and there are third-party tools that allow authentication by using the SID rather than the account name. This capability means that even if you rename the Administrator account, an attacker could launch a brute force attack by using the SID to log on.

CCE Reference Number: CCE-37953-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'	Trivial

Vulnerability Details

This policy setting prevents users from adding new Microsoft accounts on this computer. If you select the "Users can't add Microsoft accounts" option, users will not be able to create new Microsoft accounts on this computer, switch a local account to a Microsoft account, or connect a domain account to a Microsoft account. This is the preferred option if you need to limit the use of Microsoft accounts in your enterprise. If you select the "Users can't add or log on with Microsoft accounts" option, existing Microsoft account users will not be able to log on to Windows. Selecting this option might make it impossible for an existing administrator on this computer to log on and manage the system. If you disable or do not configure this policy (recommended), users will be able to use Microsoft accounts with Windows. The recommended state for this setting is: Users can't add or log on with Microsoft accounts.

Rationale: Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used to log onto their computers will probably want to block Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

CCE Reference Number: CCE-36147-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.1.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Users can't add or log on with Microsoft accounts: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts Impact: Users will not be able to log onto the computer with their Microsoft account.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Accounts: Block Microsoft accounts' is set to 'Users can't add or log on with Microsoft accounts'

Trivial

Vulnerability Details

This policy setting prevents users from adding new Microsoft accounts on this computer. The recommended state for this setting is: Users can't add or log on with Microsoft accounts.

Rationale: Organizations that want to effectively implement identity management policies and maintain firm control of what accounts are used to log onto their computers will probably want to block Microsoft accounts. Organizations may also need to block Microsoft accounts in order to meet the requirements of compliance standards that apply to their information systems.

CCE Reference Number: CCE-36147-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.1.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Users can't add or log on with Microsoft accounts:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Block Microsoft accounts>

Impact: Users will not be able to log onto the computer with their Microsoft account.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system. Note that this setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings. The recommended state for this setting is: Disabled.

Rationale: The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network, which could lead to the exposure or corruption of data.

CCE Reference Number: CCE-37432-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.1.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status Impact: All network users will need to authenticate before they can access shared resources. If you disable the Guest account and the Network Access: Sharing and Security Model option is set to Guest Only, network logons, such as those performed by the Microsoft Network Server (SMB Service), will fail. This policy setting should have little impact on most organizations because it is the default setting in Microsoft Windows 2000, Windows XP, and Windows Server#x2122; 2003.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Accounts: Guest account status' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Guest account status>

Impact: All network users will need to authenticate before they can access shared resources. If you disable the Guest account and the Network Access: Sharing and Security Model option is set to Guest Only, network logons, such as those performed by the Microsoft Network Server (SMB Service), will fail. This policy setting should have little impact on most organizations because it is the default setting in Microsoft Windows 2000, Windows XP, and Windows Server 2003.

Vulnerability Details

This policy setting determines whether the Guest account is enabled or disabled. The Guest account allows unauthenticated network users to gain access to the system. The recommended state for this setting is: Disabled. Note: This setting will have no impact when applied to the domain controller organizational unit via group policy because domain controllers have no local account database. It can be configured at the domain level via group policy, similar to account lockout and password policy settings.

Rationale: The default Guest account allows unauthenticated network users to log on as Guest with no password. These unauthorized users could access any resources that are accessible to the Guest account over the network. This capability means that any network shares with permissions that allow access to the Guest account, the Guests group, or the Everyone group will be accessible over the network, which could lead to the exposure or corruption of data.

CCE Reference Number: CCE-37432-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.1.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer. The recommended state for this setting is: Enabled.

Rationale: Blank passwords are a serious threat to computer security and should be forbidden through both organizational policy and suitable technical measures. In fact, the default settings for Active Directory domains require complex passwords of at least seven characters. However, if users with the ability to create new accounts bypass your domain-based password policies, they could create accounts with blank passwords.

For example, a user could build a stand-alone computer, create one or more accounts with blank passwords, and then join the computer to the domain. The local accounts with blank passwords would still function. Anyone who knows the name of one of these unprotected accounts could then use it to log on.

CCE Reference Number: CCE-37615-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.1.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Limit local account use of blank passwords to console logon only Impact: None. This is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Accounts: Limit local account use of blank passwords to console logon only' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. If you enable this policy setting, local accounts that have blank passwords will not be able to log on to the network from remote client computers. Such accounts will only be able to log on at the keyboard of the computer. The recommended state for this setting is: Enabled.

Rationale: Blank passwords are a serious threat to computer security and should be forbidden through both organizational policy and suitable technical measures. In fact, the default settings for Active Directory domains require complex passwords of at least seven characters. However, if users with the ability to create new accounts bypass your domain-based password policies, they could create accounts with blank passwords.

For example, a user could build a stand-alone computer, create one or more accounts with blank passwords, and then join the computer to the domain. The local accounts with blank passwords would still function. Anyone who knows the name of one of these unprotected accounts could then use it to log on.

CCE Reference Number: CCE-37615-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.1.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Accounts: Limit local account use of blank passwords to console logon only>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' — Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system Impact: There should be little or no impact because the Act as part of the operating system user right is rarely needed by any accounts other than the Local System account.

Vulnerability Details

This policy setting allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access. The recommended state for this setting is: No One.

Rationale: The Act as part of the operating system user right is extremely powerful. Anyone with this user right can take complete control of the computer and erase evidence of their activities.

CCE Reference Number: CCE-36876-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.3

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Act as part of the operating system' is set to 'No One' | Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Act as part of the operating system>

Impact: There should be little or no impact because the Act as part of the operating system user right is rarely needed by any accounts other than the Local System account.

Vulnerability Details

This policy setting allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access. The recommended state for this setting is: No One.

Rationale: The Act as part of the operating system user right is extremely powerful. Anyone with this user right can take complete control of the computer and erase evidence of their activities.

CCE Reference Number: CCE-36876-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Add workstations to domain' is set to 'Administrators' (DC only)	Trivial

Vulnerability Details

This policy setting specifies which users can add computer workstations to a specific domain. For this policy setting to take effect, it must be assigned to the user as part of the Default Domain Controller Policy for the domain. A user who has been assigned this right can add up to 10 workstations to the domain. Users who have been assigned the Create Computer Objects permission for an OU or the Computers container in Active Directory can add an unlimited number of computers to the domain, regardless of whether they have been assigned the Add workstations to a domain user right. By default, all users in the Authenticated Users group have the ability to add up to 10 computer accounts to an Active Directory domain. These new computer accounts are created in the Computers container. In Windows-based networks, the term security principal is defined as a user, group, or computer that is automatically assigned a security identifier to control access to resources. In an Active Directory domain, each computer account is a full security principal with the ability to authenticate and access domain resources. However, some organizations may want to limit the number of computers in an Active Directory environment so that they can consistently track, build, and manage the computers. If users are allowed to add computers to the domain, tracking and management efforts would be hampered. Also, users could perform activities that are more difficult to trace because of their ability to create additional unauthorized domain computers. The recommended state for this setting is: Administrators.

Rationale: The Add workstations to domain user right presents a moderate vulnerability. Users with this right could add a computer to the domain that is configured in a way that violates organizational security policies. For example, if your organization does not want its users to have administrative privileges on their computers, a user could install Windows on his or her computer and then add the computer to the domain. The user would know the password for the local administrator account, and could log on with that account and then add his or her domain account to the local Administrators group.

CCE Reference Number: CCE-36282-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Add workstations to domain>

Impact: For organizations that have never allowed users to set up their own computers and add them to the domain, this countermeasure will have no impact. For those that have allowed some or all users to configure their own computers, this countermeasure will force the organization to establish a formal process for these procedures going forward. It will not affect existing computers unless they are removed from and re-added to the domain.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process Impact: Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Adjust memory quotas for a process user right to additional accounts that are required by those components. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

Vulnerability Details

This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial of service (DoS) attack. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE.

Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Rationale: A user with the Adjust memory quotas for a process privilege can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. In the wrong hands, this privilege could be used to start a denial of service (DoS) attack.

CCE Reference Number: CCE-37071-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Adjust memory quotas for a process' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Adjust memory quotas for a process>

Impact: Organizations that have not restricted users to roles with limited privileges will find it difficult to impose this countermeasure. Also, if you have installed optional components such as ASP.NET or IIS, you may need to assign the Adjust memory quotas for a process user right to additional accounts that are required by those components. Otherwise, this countermeasure should have no impact on most computers. If this user right is necessary for a user account, it can be assigned to a local computer account instead of a domain account.

Vulnerability Details

This policy setting allows a user to adjust the maximum amount of memory that is available to a process. The ability to adjust memory quotas is useful for system tuning, but it can be abused. In the wrong hands, it could be used to launch a denial of service (DoS) attack. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE.

Note: A Member Server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #2: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale: A user with the Adjust memory quotas for a process privilege can reduce the amount of memory that is available to any process, which could cause business-critical network applications to become slow or to fail. In the wrong hands, this privilege could be used to start a denial of service (DoS) attack.

CCE Reference Number: CCE-37071-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow a Windows app to share application data between users' is set to 'Disabled' — Trivial

Vulnerability Details

Manages a Windows app's ability to share data between users who have installed the app. Data is shared through the Shared Local folder. This folder is available through the Windows.Storage API. The recommended state for this setting is: Disabled.

Rationale: Users of a system could accidentally share sensitive data with other users on the same system. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.4.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\App Package Deployment\Allow a Windows app to share application data between users>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' — Trivial

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client. If you enable this policy setting, the WinRM service will accept Basic authentication from a remote client. If you disable or do not configure this policy setting, the WinRM service will not accept Basic authentication from a remote client. The recommended state for this setting is: Disabled.

Rationale: Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

CCE Reference Number: CCE-36254-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.81.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication Impact: None - this is the default behavior.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' Trivial

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication. If you enable this policy setting, the WinRM client will use Basic authentication. If WinRM is configured to use HTTP transport, then the user name and password are sent over the network as clear text. If you disable or do not configure this policy setting, then the WinRM client will not use Basic authentication. The recommended state for this setting is: Disabled.

Rationale: Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

CCE Reference Number: CCE-36310-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.81.1.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic authentication Impact: None - this is the default behavior.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow Basic authentication>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service accepts Basic authentication from a remote client. The recommended state for this setting is: Disabled.

Rationale: Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

CCE Reference Number: CCE-36254-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.86.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Basic authentication' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow Basic authentication>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client uses Basic authentication. The recommended state for this setting is: Disabled.

Rationale: Basic authentication is less robust than other authentication methods available in WinRM because credentials including passwords are transmitted in plain text. An attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

CCE Reference Number: CCE-36310-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.86.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Cortana above lock screen' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana above lock screen

Note: This Group Policy path does not exist by default. An updated Group Policy template (Search.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: The system will need to be unlocked for the user to interact with Cortana using speech.

Vulnerability Details

This policy setting determines whether or not the user can interact with Cortana using speech while the system is locked. The recommended state for this setting is: Disabled.

Rationale: Access to any computer resource should not be allowed when the device is locked. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.54.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Cortana' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow Cortana

Note: This Group Policy path does not exist by default. An updated Group Policy template (Search.admx/adml) is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: Cortana will be turned off. Users will still be able to use search to find things on the device and on the Internet.

Vulnerability Details

This policy setting specifies whether Cortana is allowed on the device. The recommended state for this setting is: Disabled.

Rationale: If Cortana is enabled, sensitive information could be contained in search history and sent out to Microsoft. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.54.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Extensions' is set to 'Disabled'	Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Allow Extensions>

Impact: Employees will not be able to use Edge Extensions.

Vulnerability Details

This setting lets you decide whether employees can load extensions in Microsoft Edge. The recommended state for this setting is: Disabled.

Rationale: To prevent malicious extensions from being loaded, only approved extensions should be installed. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of encrypted files Note: This Group Policy path does not exist by default. An additional Group Policy template (Search.admx/adml) is required - it is included with the Microsoft Windows Vista, 2008, 7/2008R2, 8/2012, 8.1/2012R2 and Windows 10 Administrative Templates.

Impact: The search service components (including non-Microsoft components) will not encrypted items or encrypted stores.

Vulnerability Details

This policy setting allows encrypted items to be indexed. If you enable this policy setting, indexing will attempt to decrypt and index the content (access restrictions will still apply). If you disable this policy setting, the search service components (including non-Microsoft components) are expected not to index encrypted items or encrypted stores. This policy setting is not configured by default. If you do not configure this policy setting, the local setting, configured through Control Panel, will be used. By default, the Control Panel setting is set to not index encrypted content. When this setting is enabled or disabled, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files. The recommended state for this setting is: Disabled.

Rationale: Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

CCE Reference Number: CCE-38277-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.50.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow indexing of encrypted files' is set to 'Disabled'

Trivial

Vulnerability Details

This policy setting controls whether encrypted items are allowed to be indexed. When this setting is changed, the index is rebuilt completely. Full volume encryption (such as BitLocker Drive Encryption or a non-Microsoft solution) must be used for the location of the index to maintain security for encrypted files. The recommended state for this setting is: Disabled.

Rationale: Indexing and allowing users to search encrypted files could potentially reveal confidential data stored within the encrypted files.

CCE Reference Number: CCE-38277-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.54.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow indexing of encrypted files

Note: This Group Policy path does not exist by default. An additional Group Policy template (Search.admx/adml) is required - it is included with the Microsoft Windows Vista, 2008, 7/2008R2, 8/2012, 8.1/2012R2 and Windows 10 Administrative Templates.

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow InPrivate Browsing' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Allow InPrivate Browsing>

Impact: Employees will not be able to use InPrivate website browsing.

Vulnerability Details

This setting lets you decide whether employees can browse using InPrivate website browsing. The recommended state for this setting is: Disabled.

Rationale: Even though web filter logs can monitor traffic to and from websites, it is always a good practice to try and keep multiple source of logs. It can also be helpful to keep user from privately browsing in order to troubleshoot malicious site visits if a machine has become compromised.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Input Personalization' is set to 'Disabled' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Control Panel\Regional and Language Options\Allow Input Personalization>

Impact: Automatic learning of speech, inking, and typing stops and users cannot change its value via PC Settings.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy enables the automatic learning component of input personalization that includes speech, inking, and typing. Automatic learning enables the collection of speech and handwriting patterns, typing history, contacts, and recent calendar information. It is required for the use of Cortana. Some of this collected information may be stored on the user's OneDrive, in the case of inking and typing; some of the information will be uploaded to Microsoft to personalize speech. The recommended state for this setting is: Disabled.

Rationale: If this setting is Enabled sensitive information could be stored in the cloud or sent to Microsoft. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.1.2.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Allow Microsoft accounts to be optional Impact: Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead.

Vulnerability Details

This policy setting lets you control whether Microsoft accounts are optional for Windows Store apps that require an account to sign in. This policy only affects Windows Store apps that support it. If you enable this policy setting, Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead. If you disable or do not configure this policy setting, users will need to sign in with a Microsoft account. The recommended state for this setting is: Enabled.

Rationale: Enabling this setting allows an organization to use their enterprise user accounts instead of using their Microsoft accounts when accessing Windows store apps. This provides the organization with greater control over relevant credentials. Microsoft accounts cannot be centrally managed and as such enterprise credential security policies cannot be applied to them, which could put any information accessed by using Microsoft accounts at risk.

CCE Reference Number: CCE-38354-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.6.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Microsoft accounts to be optional' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting lets you control whether Microsoft accounts are optional for Windows Store apps that require an account to sign in. This policy only affects Windows Store apps that support it. The recommended state for this setting is: Enabled.

Rationale: Enabling this setting allows an organization to use their enterprise user accounts instead of using their Microsoft accounts when accessing Windows store apps. This provides the organization with greater control over relevant credentials. Microsoft accounts cannot be centrally managed and as such enterprise credential security policies cannot be applied to them, which could put any information accessed by using Microsoft accounts at risk.

CCE Reference Number: CCE-38354-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.6.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Allow Microsoft accounts to be optional>

Impact: Windows Store apps that typically require a Microsoft account to sign in will allow users to sign in with an enterprise account instead.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow network connectivity during connected-standby (on battery)' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (on battery)

Note: This Group Policy path does not exist by default. An updated Group Policy template (Power.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: Network connectivity in standby (while on battery) is not guaranteed. This connectivity restriction currently only applies to WLAN networks only, but is subject to change (according to Microsoft).

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems. The recommended state for this setting is: Disabled.

Rationale: Disabling this setting ensures that the computer will not be accessible to attackers over a WLAN network while left unattended, on battery and in a sleep state.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.29.5.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow network connectivity during connected-standby (plugged in)' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Allow network connectivity during connected-standby (plugged in)

Note: This Group Policy path does not exist by default. An updated Group Policy template (Power.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: Network connectivity in standby (while plugged in) is not guaranteed. This connectivity restriction currently only applies to WLAN networks only, but is subject to change (according to Microsoft).

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting allows you to control the network connectivity state in standby on modern standby-capable systems. The recommended state for this setting is: Disabled.

Rationale: Disabling this setting ensures that the computer will not be accessible to attackers over a WLAN network while left unattended, plugged in and in a sleep state.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.29.5.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow remote server management through WinRM' is set to 'Disabled' — Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled:

<Computer Configuration\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow remote server management through WinRM>

Impact: None - this is the default behavior.

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service automatically listens on the network for requests on the HTTP transport over the default HTTP port. The recommended state for this setting is: Disabled.

Rationale: Any feature is a potential avenue of attack, those that enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Management (WinRM) service on trusted networks and when feasible employ additional controls such as IPsec.

CCE Reference Number: CCE-37927-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.86.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Remote Shell Access' is set to 'Disabled' — Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled:

<Computer Configuration\Administrative Templates\Windows Components\Windows Remote Shell\Allow Remote Shell Access>

Impact: New Remote Shell connections are not allowed and are rejected by the server.

Note: On Server 2012 (non-R2) and higher, due to design changes in the OS after Server 2008 R2, configuring this setting as prescribed will prevent the ability to add or remove Roles and Features (even locally) via the GUI. We therefore recommend that the necessary Roles and Features be installed prior to configuring this setting on a Level 2 server. Alternatively, Roles and Features can still be added or removed using the PowerShell commands Add-WindowsFeature or Remove-WindowsFeature in the Server Manager module, even with this setting configured.

Vulnerability Details

This policy setting allows you to manage configuration of remote access to all supported shells to execute scripts and commands. The recommended state for this setting is: Disabled.

Note: The GPME help text for this setting is incorrectly worded, implying that configuring it to Enabled will reject new remote shell connections, and setting it to Disabled will allow remote shell connections. The opposite is true (and is consistent with the title of the setting). This is a wording mistake by Microsoft in the Administrative Template.

Rationale: Any feature is a potential avenue of attack, those that enable inbound network connections are particularly risky. Only enable the use of the Windows Remote Shell on trusted networks and when feasible employ additional controls such as IPsec.

CCE Reference Number: CCE-36499-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.87.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow search and Cortana to use location' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Search\Allow search and Cortana to use location

Note: This Group Policy path does not exist by default. An updated Group Policy template (Search.admx/adml) is required - it is included with the Microsoft Windows 10 Administrative Templates.

Impact: Search and Cortana will not have access to location information.

Vulnerability Details

This policy setting specifies whether search and Cortana can provide location aware search and Cortana results. The recommended state for this setting is: Disabled.

Rationale: In an Enterprise having Cortana and Search having access to location is unnecessary. Organizations may not want this information shared out.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.54.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow suggested apps in Windows Ink Workspace' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Ink Workspace\Allow suggested apps in Windows Ink Workspace

Note: This Group Policy path does not exist by default. An updated Group Policy template (WindowsInkWorkspace.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: The suggested apps in Windows Ink Workspace will not be allowed.

Vulnerability Details

This policy setting determines whether suggested apps in Windows Ink Workspace are allowed. The recommended state for this setting is: Disabled.

Rationale: Disabling this setting will help ensure your data is not shared with any third party. The Microsoft feature will collect data and suggested apps based on that data collected.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.73.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Telemetry' is set to 'Enabled: 0 - Security [Enterprise Only]' — Trivial

Vulnerability Details

This policy setting determines the amount of diagnostic and usage data reported to Microsoft. A value of 0 will send minimal data to Microsoft. This data includes Malicious Software Removal Tool (MSRT) & Windows Defender data, if enabled, and telemetry client settings. Setting a value of 0 applies to enterprise, EDU, IoT and server devices only. Setting a value of 0 for other devices is equivalent to choosing a value of 1. A value of 1 sends only a basic amount of diagnostic and usage data.

Note that setting values of 0 or 1 will degrade certain experiences on the device. A value of 2 sends enhanced diagnostic and usage data. A value of 3 sends the same data as a value of 2, plus additional diagnostics data, including the files and content that may have caused the problem. Windows 10 telemetry settings apply to the Windows operating system and some first party apps. This setting does not apply to third party apps running on Windows 10. The recommended state for this setting is: Enabled: 0 - Security [Enterprise Only]. Note: If the "Allow Telemetry" setting is configured to "0 - Security [Enterprise Only]", then the options in Windows Update to defer upgrades and updates will have no effect.

Rationale: Sending any data to a 3rd party vendor is a security concern and should only be done on an as needed basis. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.16.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 0 - Security [Enterprise Only]: Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Allow Telemetry

Note: This Group Policy path does not exist by default. An additional Group Policy template (datacollection.admx/adml) is required - it is included with the Microsoft Windows 10 Administrative Templates.

Impact: Note that setting values of 0 or 1 will degrade certain experiences on the device.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' — Trivial

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled.

Rationale: Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

CCE Reference Number: CCE-38223-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.81.2.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic Impact: None - this is the default behavior.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic Impact: None - this is the default behavior.

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network. If you enable this policy setting, the WinRM client sends and receives unencrypted messages over the network. If you disable or do not configure this policy setting, the WinRM client sends or receives only encrypted messages over the network. The recommended state for this setting is: Disabled.

Rationale: Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying

WinRM messages as they transit the network.

CCE Reference Number: CCE-37726-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.81.1.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' — Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Allow unencrypted traffic>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service sends and receives unencrypted messages over the network. The recommended state for this setting is: Disabled.

Rationale: Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

CCE Reference Number: CCE-38223-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.86.2.3

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow unencrypted traffic' is set to 'Disabled' Trivial

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client sends and receives unencrypted messages over the network. The recommended state for this setting is: Disabled.

Rationale: Encrypting WinRM network traffic reduces the risk of an attacker viewing or modifying WinRM messages as they transit the network.

CCE Reference Number: CCE-37726-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.86.1.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Allow unencrypted traffic>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Use of Camera' is set to 'Disabled' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Camera\Allow Use of Camera

Note: This Group Policy path does not exist by default. An updated Group Policy template (Camera.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: Users will not be able to utilize the camera on a system.

Vulnerability Details

This policy setting controls whether the use of Camera devices on the machine are permitted. The recommended state for this setting is: Disabled.

Rationale: Cameras in a high security environment can pose serious privacy and data exfiltration risks - they should be disabled to help mitigate that risk.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.12.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Allow user control over installs Impact: If you disable or do not configure this policy setting, the security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Permits users to change installation options that typically are available only to system administrators. The security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user. The recommended state for this setting is: Disabled.

Rationale: In an Enterprise environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability can risk unapproved software from being installed our removed from a system which could cause the system to become vulnerable.

CCE Reference Number: CCE-36400-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.69.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow user control over installs' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Allow user control over installs>

Impact: None - this is the default configuration.

Vulnerability Details

Permits users to change installation options that typically are available only to system administrators. The security features of Windows Installer prevent users from changing installation options typically reserved for system administrators, such as specifying the directory to which files are installed. If Windows Installer detects that an installation package has permitted the user to change a protected option, it stops the installation and displays a message. These security features operate only when the installation program is running in a privileged security context in which it has access to directories denied to the user. The recommended state for this setting is: Disabled.

Rationale: In an Enterprise environment, only IT staff with administrative rights should be installing or changing software on a system. Allowing users the ability can risk unapproved software from being installed our removed from a system which could cause the system to become vulnerable.

CCE Reference Number: CCE-36400-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.74.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Allow Windows Ink Workspace' is set to 'Enabled: On, but disallow access above lock' OR 'Disabled' but not 'Enabled: On'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: On, but disallow access above lock OR Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Ink Workspace\Allow Windows Ink Workspace

Note: This Group Policy path does not exist by default. An updated Group Policy template (WindowsInkWorkspace.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Impact: Windows Ink Workspace will not be permitted above the lock screen.

Vulnerability Details

This policy setting determines whether Windows Ink items are allowed above the lock screen. The recommended state for this setting is: Enabled: On, but disallow access above lock OR Disabled.

Rationale: Allowing any apps to be accessed while system is locked is not recommended. If this feature is permitted, it should only be accessible once a user authenticates with the proper credentials. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.73.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled'

Trivial

Vulnerability Details

Directs Windows Installer to use system permissions when it installs any program on the system. This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers. If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer.
Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders.

Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: Disabled.

Rationale: Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

CCE Reference Number: CCE-37490-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 19.7.37.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: User Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges Impact: Windows Installer will apply the current user's permissions when it installs programs, this will prevent standard users from installing applications that affect system-wide configuration items.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' — Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges Impact: Windows Installer will apply the current user's permissions when it installs programs, this will prevent standard users from installing applications that affect system-wide configuration items.

Vulnerability Details

Directs Windows Installer to use system permissions when it installs any program on the system. This setting extends elevated privileges to all programs. These privileges are usually reserved for programs that have been assigned to the user (offered on the desktop), assigned to the computer (installed automatically), or made available in Add or Remove Programs in Control Panel. This setting lets users install programs that require access to directories that the user might not have permission to view or change, including directories on highly restricted computers. If you disable this setting or do not configure it, the system applies the current user's permissions when it installs programs that a system administrator does not distribute or offer.

Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders. Caution: Skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: Disabled.

Rationale: Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

CCE Reference Number: CCE-36919-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.69.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Always install with elevated privileges' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Always install with elevated privileges>

Impact: None - this is the default configuration.

Vulnerability Details

This setting controls whether or not Windows Installer should use system permissions when it installs any program on the system.

Note: This setting appears both in the Computer Configuration and User Configuration folders. To make this setting effective, you must enable the setting in both folders.

Caution: If enabled, skilled users can take advantage of the permissions this setting grants to change their privileges and gain permanent access to restricted files and folders. Note that the User Configuration version of this setting is not guaranteed to be secure. The recommended state for this setting is: Disabled.

Rationale: Users with limited privileges can exploit this feature by creating a Windows Installer installation package that creates a new local account that belongs to the local built-in Administrators group, adds their current account to the local built-in Administrators group, installs malicious software, or performs other unauthorized activities.

CCE Reference Number: CCE-36919-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.74.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection Impact: Users will always have to enter their password when they establish new Terminal Server sessions.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting specifies whether Terminal Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. By default, Terminal Services allows users to automatically log on if they enter a password in the Remote Desktop Connection client.

Note: If you do not configure this policy setting, the local computer administrator can use the Terminal Services Configuration tool to either allow or prevent passwords from being automatically sent. The recommended state for this setting is: Enabled.

Rationale: Users have the option to store both their username and password when they create a new Remote Desktop connection shortcut. If the server that runs Terminal Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Terminal Server through the Remote Desktop connection shortcut, even though they may not know the user's password.

CCE Reference Number: CCE-37929-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.48.3.9.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Always prompt for password upon connection' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting specifies whether Terminal Services always prompts the client computer for a password upon connection. You can use this policy setting to enforce a password prompt for users who log on to Terminal Services, even if they already provided the password in the Remote Desktop Connection client. The recommended state for this setting is: Enabled.

Rationale: Users have the option to store both their username and password when they create a new Remote Desktop connection shortcut. If the server that runs Terminal Services allows users who have used this feature to log on to the server but not enter their password, then it is possible that an attacker who has gained physical access to the user's computer could connect to a Terminal Server through the Remote Desktop connection shortcut, even though they may not know the user's password.

CCE Reference Number: CCE-37929-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.9.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Always prompt for password upon connection>

Impact: Users cannot automatically log on to Terminal Services by supplying their passwords in the Remote Desktop Connection client. They will be prompted for a password to log on.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Vulnerability Details

This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled.

Note: Old events may or may not be retained according to the "Backup log automatically when full" policy setting.

Rationale: If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37775-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.24.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Application: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Control Event Log behavior when the log file reaches its maximum size>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting controls Event Log behavior when the log file reaches its maximum size. The recommended state for this setting is: Disabled.

Note: Old events may or may not be retained according to the "Backup log automatically when full" policy setting.

Rationale: If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37775-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.26.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Trivial

Vulnerability Details

This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37948-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.24.1.2

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed. The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data. Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Application: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Application\Specify the maximum log file size (KB)>

Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed. The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data. Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Vulnerability Details

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. The recommended state for this setting is: Enabled: 32,768 or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37948-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.26.1.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only) — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\Apply UAC restrictions to local accounts on network logons

Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).
Impact: None - this is the default behavior.

Vulnerability Details

This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk. Enabled: Applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the LocalAccountTokenFilterPolicy registry value to 0. This is the default behavior for Windows. Disabled: Allows local accounts to have full administrative rights when authenticating via network logon, by configuring the LocalAccountTokenFilterPolicy registry value to 1. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about LocalAccountTokenFilterPolicy, see Microsoft Knowledge Base article 951016: Description of User Account Control and remote restrictions in Windows Vista. The recommended state for this setting is: Enabled.

Rationale: Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Ensuring this policy is Enabled significantly reduces that risk.

CCE Reference Number: CCE-37069-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.6.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Apply UAC restrictions to local accounts on network logons' is set to 'Enabled' (MS only)

Trivial

Vulnerability Details

This setting controls whether local accounts can be used for remote administration via network logon (e.g., NET USE, connecting to C$, etc.). Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Enabling this policy significantly reduces that risk.

Enabled: Applies UAC token-filtering to local accounts on network logons. Membership in powerful group such as Administrators is disabled and powerful privileges are removed from the resulting access token. This configures the LocalAccountTokenFilterPolicy registry value to 0. This is the default behavior for Windows.

Disabled: Allows local accounts to have full administrative rights when authenticating via network logon, by configuring the LocalAccountTokenFilterPolicy registry value to 1. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about LocalAccountTokenFilterPolicy, see Microsoft Knowledge Base article 951016: Description of User Account Control and remote restrictions in Windows Vista. The recommended state for this setting is: Enabled.

Rationale: Local accounts are at high risk for credential theft when the same account and password is configured on multiple systems. Ensuring this policy is Enabled significantly reduces that risk.

CCE Reference Number: CCE-37069-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.6.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\Apply UAC restrictions to local accounts on network logons

Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Account Lockout' is set to 'Success' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports when a user's account is locked out as a result of too many failed logon attempts. Events for this subcategory include: 4625: An account failed to log on. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37133-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.5.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Account Lockout' is set to 'Success and Failure'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Account Lockout>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports when a user's account is locked out as a result of too many failed logon attempts. Events for this subcategory include: 4625: An account failed to log on. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37133-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.5.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Application Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This policy setting allows you to audit events generated by changes to application groups such as the following: Application group is created, changed, or deleted. Member is added or removed from an application group. Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at MSDN - Windows Authorization Manager. The recommended state for this setting is: Success and Failure .

Rationale: Auditing events in this category may be useful when investigating an incident.

CCE Reference Number: CCE-38329-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Application Group Management' is set to 'Success and Failure'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Application Group Management>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This policy setting allows you to audit events generated by changes to application groups such as the following: Application group is created, changed, or deleted. Member is added or removed from an application group. Application groups are utilized by Windows Authorization Manager, which is a flexible framework created by Microsoft for integrating role-based access control (RBAC) into applications. More information on Windows Authorization Manager is available at MSDN - Windows Authorization Manager. The recommended state for this setting is: Success and Failure.

Rationale: Auditing events in this category may be useful when investigating an incident.

CCE Reference Number: CCE-38329-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure'

Trivial

Vulnerability Details

This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include: 4715: The audit policy (SACL) on an object was changed. 4719: System audit policy was changed. 4902: The Per-user audit policy table was created. 4904: An attempt was made to register a security event source. 4905: An attempt was made to unregister a security event source. 4906: The CrashOnAuditFail value has changed. 4907: Auditing settings on object were changed. 4908: Special Groups Logon table modified. 4912: Per User Audit Policy was changed. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38028-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.7.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Audit Policy Change' is set to 'Success and Failure' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Audit Policy Change>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and

computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports changes in audit policy including SACL changes. Events for this subcategory include: 4715: The audit policy (SACL) on an object was changed. 4719: System audit policy was changed. 4902: The Per-user audit policy table was created. 4904: An attempt was made to register a security event source. 4905: An attempt was made to unregister a security event source. 4906: The CrashOnAuditFail value has changed. 4907: Auditing settings on object were changed. 4908: Special Groups Logon table modified. 4912: Per User Audit Policy was changed. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38028-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.7.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication Policy Change Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This subcategory reports changes in authentication policy. Events for this subcategory include: 4706: A new trust was created to a domain. 4707: A trust to a domain was removed. 4713: Kerberos policy was changed. 4716: Trusted domain information was modified. 4717: System security access was granted to an account. 4718: System security access was removed from an account. 4739: Domain Policy was changed. 4864: A namespace collision was detected. 4865: A trusted forest information entry was added. 4866: A trusted forest information entry was removed. 4867: A trusted forest information entry was modified. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38327-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.7.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Authentication Policy Change' is set to 'Success' — Trivial

Vulnerability Details

This subcategory reports changes in authentication policy. Events for this subcategory include: 4706: A new trust was created to a domain. 4707: A trust to a domain was removed. 4713: Kerberos policy was changed. 4716: Trusted domain information was modified. 4717: System security access was granted to an account. 4718: System security access was removed from an account. 4739: Domain Policy was changed. 4864: A namespace collision was detected. 4865: A trusted forest information entry was added. 4866: A trusted forest information entry was removed. 4867: A trusted forest information entry was modified. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38327-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.7.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authentication Policy Change>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Authorization Policy Change' is set to 'Success'

Trivial

Vulnerability Details

This subcategory reports changes in authorization policy. Events for this subcategory include: 4704: A user right was assigned. 4705: A user right was removed. 4706: A new trust was created to a domain. 4707: A trust to a domain was removed. 4714: Encrypted data recovery policy was changed. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36320-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.7.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Policy Change\Audit Authorization Policy Change>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Computer Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include: 4741: A computer account was created. 4742: A computer account was changed. 4743: A computer account was deleted. The recommended state for this setting is: Success and Failure.

Rationale: Auditing events in this category may be useful when investigating an incident.

CCE Reference Number: CCE-38004-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Audit Computer Account Management' is set to 'Success and Failure' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Computer Account Management>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This subcategory reports each event of computer account management, such as when a computer account is created, changed, deleted, renamed, disabled, or enabled. Events for this subcategory include: 4741: A computer account was created. 4742: A computer account was changed. 4743: A computer account was deleted. The recommended state for this setting is: Success and Failure.

Rationale: Auditing events in this category may be useful when investigating an incident.

CCE Reference Number: CCE-38004-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.2.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the

Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include: 4774: An account was mapped for logon. 4775: An account could not be mapped for logon. 4776: The domain controller attempted to validate the credentials for an account. 4777: The domain controller failed to validate the credentials for an account. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37741-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Credential Validation' is set to 'Success and Failure'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Logon\Audit Credential Validation>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and

computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports the results of validation tests on credentials submitted for a user account logon request. These events occur on the computer that is authoritative for the credentials. For domain accounts, the domain controller is authoritative, whereas for local accounts, the local computer is authoritative. In domain environments, most of the Account Logon events occur in the Security log of the domain controllers that are authoritative for the domain accounts. However, these events can occur on other computers in the organization when local accounts are used to log on. Events for this subcategory include: 4774: An account was mapped for logon. 4775: An account could not be mapped for logon. 4776: The domain controller attempted to validate the credentials for an account. 4777: The domain controller failed to validate the credentials for an account. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37741-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Directory Service Access' is set to 'Success and Failure' (DC only)

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Access>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and

computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports when an AD DS object is accessed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. These events are similar to the directory service access events in previous versions of Windows Server. This subcategory applies only to domain controllers. Events for this subcategory include: 4662: An operation was performed on an object. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37433-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.4.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Directory Service Changes' is set to 'Success and Failure' (DC only) — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure.

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\DS Access\Audit Directory Service Changes>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports changes to objects in Active Directory Domain Services (AD DS). The types of changes that are reported are create, modify, move, and undelete operations that are performed on an object. DS Change auditing, where appropriate, indicates the old and new values of the changed properties of the objects that were changed. Only objects with SACLs cause audit events to be generated, and only when they are accessed in a manner that matches their SACL. Some objects and properties do not cause audit events to be generated due to settings on the object class in the schema. This subcategory applies only to domain controllers. Events for this subcategory include: 5136: A directory service object was modified. 5137: A directory service object was created. 5138: A directory service object was undeleted. 5139: A directory service object was moved. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37616-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.4.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Distribution Group Management' is set to 'Success and Failure' (DC only)

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Distribution Group Management>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports each event of distribution group management, such as when a distribution group is created, changed, or deleted or when a member is added to or removed from a distribution group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of group accounts. Events for this subcategory include: 4744: A security-disabled local group was created. 4745: A security-disabled local group was changed. 4746: A member was added to a security-disabled local group. 4747: A member was removed from a security-disabled local group. 4748: A security-disabled local group was deleted. 4749: A security-disabled global group was created. 4750: A security-disabled global group was changed. 4751: A member was added to a security-disabled global group. 4752: A member was removed from a security-disabled global group. 4753: A security-disabled global group was deleted. 4759: A security-disabled universal group was created. 4760: A security-disabled universal group was changed. 4761: A member was added to a security-disabled universal group. 4762: A member was removed from a security-disabled universal group. 4763: A security-disabled universal group was deleted. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may provide an organization with insight when investigating an incident. For example, when a given unauthorized user was added to a sensitive distribution group.

CCE Reference Number: CCE-36265-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.2.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings Impact: The individual audit policy subcategories that are available in Windows Vista are not exposed in the interface of Group Policy tools. Administrators can deploy a custom audit policy that applies detailed security auditing settings to Windows Vista-based client computers in a Windows Server 2003 domain or in a Windows 2000 domain. If after enabling this setting, you attempt to modify an auditing setting by using Group Policy, the Group Policy auditing setting will be ignored in favor of the custom policy setting. To modify auditing settings by using Group Policy, you must first disable this key.

Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Vulnerability Details

This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista. The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled. The recommended state for this setting is: Enabled.

Rationale: Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

CCE Reference Number: CCE-37850-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows administrators to enable the more precise auditing capabilities present in Windows Vista. The Audit Policy settings available in Windows Server 2003 Active Directory do not yet contain settings for managing the new auditing subcategories. To properly apply the auditing policies prescribed in this baseline, the Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings setting needs to be configured to Enabled. The recommended state for this setting is: Enabled.

Important: Be very cautious about audit settings that can generate a large volume of traffic. For example, if you enable either success or failure auditing for all of the Privilege Use subcategories, the high volume of audit events generated can make it difficult to find other types of entries in the Security log. Such a configuration could also have a significant impact on system performance.

Rationale: Prior to the introduction of auditing subcategories in Windows Vista, it was difficult to track events at a per-system or per-user level. The larger event categories created too many events and the key information that needed to be audited was difficult to find.

CCE Reference Number: CCE-37850-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Group Membership' is set to 'Success' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Group Membership>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This policy allows you to audit the group membership information in the users logon token. Events in this subcategory are generated on the computer on which a logon session is created. For an interactive logon, the security audit event is generated on the computer that the user logged on to. For a network logon, such as accessing a shared folder on the network, the security audit event is generated on the computer hosting the resource. The recommended state for this setting is: Success.

Note: A Windows 10, Server 2016 or higher OS is required to access and set this value in Group Policy.

Rationale: Auditing these events may be useful when investigating a security incident.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.5.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include: 4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations. 4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer. 4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay. 4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt. 4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored. 5478: IPsec Services has started successfully. 5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks. 5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. 5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started. 5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks. 5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37853-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.9.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit IPsec Driver' is set to 'Success and Failure' Trivial

Vulnerability Details

This subcategory reports on the activities of the Internet Protocol security (IPsec) driver. Events for this subcategory include: 4960: IPsec dropped an inbound packet that failed an integrity check. If this problem persists, it could indicate a network issue or that packets are being modified in transit to this computer. Verify that the packets sent from the remote computer are the same as those received by this computer. This error might also indicate interoperability problems with other IPsec implementations. 4961: IPsec dropped an inbound packet that failed a replay check. If this problem persists, it could indicate a replay attack against this computer. 4962: IPsec dropped an inbound packet that failed a replay check. The inbound packet had too low a sequence number to ensure it was not a replay. 4963: IPsec dropped an inbound clear text packet that should have been secured. This is usually due to the remote computer changing its IPsec policy without informing this computer. This could also be a spoofing attack attempt. 4965: IPsec received a packet from a remote computer with an incorrect Security Parameter Index (SPI). This is usually caused by malfunctioning hardware that is corrupting packets. If these errors persist, verify that the packets sent from the remote computer are the same as those received by this computer. This error may also indicate interoperability problems with other

IPsec implementations. In that case, if connectivity is not impeded, then these events can be ignored. 5478: IPsec Services has started successfully. 5479: IPsec Services has been shut down successfully. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks. 5480: IPsec Services failed to get the complete list of network interfaces on the computer. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. 5483: IPsec Services failed to initialize RPC server. IPsec Services could not be started. 5484: IPsec Services has experienced a critical failure and has been shut down. The shutdown of IPsec Services can put the computer at greater risk of network attack or expose the computer to potential security risks. 5485: IPsec Services failed to process some IPsec filters on a plug-and-play event for network interfaces. This poses a potential security risk because some of the network interfaces may not get the protection provided by the applied IPsec filters. Use the IP Security Monitor snap-in to diagnose the problem. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37853-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.9.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit IPsec Driver>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Logoff' is set to 'Success' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports when a user logs off from the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include: 4634: An account was logged off. 4647: User initiated logoff. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38237-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.5.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Logoff' is set to 'Success' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logoff>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and

computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports when a user logs off from the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include: 4634: An account was logged off. 4647: User initiated logoff. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38237-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.5.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports when a user attempts to log on to the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include: 4624: An account was successfully logged on. 4625: An account failed to log on. 4648: A logon was attempted using explicit credentials. 4675: SIDs were filtered. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38036-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.5.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Logon' is set to 'Success and Failure' — Trivial

Vulnerability Details

This subcategory reports when a user attempts to log on to the system. These events occur on the accessed computer. For interactive logons, the generation of these events occurs on the computer that is logged on to. If a network logon takes place to access a share, these events generate on the computer that hosts the accessed resource. If you configure this setting to No auditing, it is difficult or impossible to determine which user has accessed or attempted to access organization computers. Events for this subcategory include: 4624: An account was successfully logged on. 4625: An account failed to log on. 4648: A logon was attempted using explicit credentials. 4675: SIDs were filtered. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38036-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.5.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Logon>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Other Account Management Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports other account management events. Events for this subcategory include: 4782: The password hash an account was accessed. 4793: The Password Policy Checking API was called. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37855-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.2.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Audit Other Account Management Events' is set to 'Success and Failure' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Other Account Management Events>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports other account management events. Events for this subcategory include: 4782: The password hash an account was accessed. 4793: The Password Policy Checking API was called. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37855-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.2.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports other logon/logoff-related events, such as Terminal Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include: 4649: A replay attack was detected. 4778: A session was reconnected to a Window Station. 4779: A session was disconnected from a Window Station. 4800: The workstation was locked. 4801: The workstation was unlocked. 4802: The screen saver was invoked. 4803: The screen saver was dismissed. 5378: The requested credentials delegation was disallowed by policy. 5632: A request was made to authenticate to a wireless network. 5633: A request was made to authenticate to a wired network. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36322-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.5.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Other Logon/Logoff Events' is set to 'Success and Failure'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Other Logon/Logoff Events>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports other logon/logoff-related events, such as Terminal Services session disconnects and reconnects, using RunAs to run processes under a different account, and locking and unlocking a workstation. Events for this subcategory include: 4649: A replay attack was detected. 4778: A session was reconnected to a Window Station. 4779: A session was disconnected from a Window Station. 4800: The workstation was locked. 4801: The workstation was unlocked. 4802: The screen saver was invoked. 4803: The screen saver was dismissed. 5378: The requested credentials delegation was disallowed by policy. 5632: A request was made to authenticate to a wireless network. 5633: A request was made to authenticate to a wired network. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36322-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.5.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' — Trivial

Vulnerability Details

This subcategory reports on other system events. Events for this subcategory include: 5024 : The Windows Firewall Service has started successfully. 5025 : The Windows Firewall Service has been stopped. 5027 : The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy. 5028 : The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy. 5029: The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy. 5030: The Windows Firewall Service failed to start. 5032: Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network. 5033 : The Windows Firewall Driver has started successfully. 5034 : The Windows Firewall Driver has been stopped. 5035 : The Windows Firewall Driver failed to start. 5037 : The Windows Firewall Driver detected critical runtime error. Terminating. 5058: Key file operation. 5059: Key migration operation. The recommended state for this setting is: Success and Failure.

Rationale: Capturing these audit events may be useful for identifying when the Windows Firewall is not performing as expected.

CCE Reference Number: CCE-38030-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.9.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Other System Events Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Other System Events' is set to 'Success and Failure' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Other System Events>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and

computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports on other system events. Events for this subcategory include: 5024 : The Windows Firewall Service has started successfully. 5025 : The Windows Firewall Service has been stopped. 5027 : The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy. 5028 : The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy. 5029: The Windows Firewall Service failed to initialize the driver. The service will continue to enforce the current policy. 5030: The Windows Firewall Service failed to start. 5032: Windows Firewall was unable to notify the user that it blocked an application from accepting incoming connections on the network. 5033 : The Windows Firewall Driver has started successfully. 5034 : The Windows Firewall Driver has been stopped. 5035 : The Windows Firewall Driver failed to start. 5037 : The Windows Firewall Driver detected critical runtime error. Terminating. 5058: Key file operation. 5059: Key migration operation. The recommended state for this setting is: Success and Failure.

Rationale: Capturing these audit events may be useful for identifying when the Windows Firewall is not performing as expected.

CCE Reference Number: CCE-38030-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.9.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit PNP Activity' is set to 'Success' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit PNP Activity>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and

computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting allows you to audit when plug and play detects an external device. The recommended state for this setting is: Success.

Note: A Windows 10, Server 2016 or higher OS is required to access and set this value in Group Policy.

Rationale: Enabling this setting will allow a user to audit events when a device is plugged into a system. This can help alert IT staff if unapproved devices are plugged in.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.3.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Process Creation' is set to 'Success' | Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include: 4688: A new process has been created. 4696: A primary token was assigned to process. Refer to Microsoft Knowledge Base article 947226: Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36059-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.3.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Process Creation' is set to 'Success'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports the creation of a process and the name of the program or user that created it. Events for this subcategory include: 4688: A new process has been created. 4696: A primary token was assigned to process. Refer to Microsoft Knowledge Base article 947226: Description of security events in Windows Vista and in Windows Server 2008 for the most recent information about this setting. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36059-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.3.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Removable Storage Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This policy setting allows you to audit user attempts to access file system objects on a removable storage device. A security audit event is generated only for all objects for all types of access requested. If you configure this policy setting, an audit event is generated each time an account accesses a file system object on a removable storage. Success audits record successful attempts and Failure audits record unsuccessful attempts. If you do not configure this policy setting, no audit event is generated when an account accesses a file system object on a removable storage. The recommended state for this setting is: Success and Failure.

Note: A Windows 8, Server 2012 (non-R2) or higher OS is required to access and set this value in Group Policy.

Rationale: Auditing removable storage may be useful when investigating an incident. For example, if an individual is suspected of copying sensitive information onto a USB drive.

CCE Reference Number: CCE-37617-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.6.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Audit Removable Storage' is set to 'Success and Failure'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Object Access\Audit Removable Storage>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This policy setting allows you to audit user attempts to access file system objects on a removable storage device. A security audit event is generated only for all objects for all types of access requested. If you configure this policy setting, an audit event is generated each time an account accesses a file system object on a removable storage. Success audits record successful attempts and Failure audits record unsuccessful attempts. If you do not configure this policy setting, no audit event is generated when an account accesses a file system object on a removable storage. The recommended state for this setting is: Success and Failure.

Note: A Windows 8, Server 2012 (non-R2) or higher OS is required to access and set this value in Group Policy.

Rationale: Auditing removable storage may be useful when investigating an incident. For example, if an individual is suspected of copying sensitive information onto a USB drive.

CCE Reference Number: CCE-37617-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.6.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Security Group Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include: 4727: A security-enabled global group was created. 4728: A member was added to a security-enabled global group. 4729: A member was removed from a security-enabled global group. 4730: A security-enabled global group was deleted. 4731: A security-enabled local group was created. 4732: A member was added to a security-enabled local group. 4733: A member was removed from a security-enabled local group. 4734: A security-enabled local group was deleted. 4735: A security-enabled local group was changed. 4737: A security-enabled global group was changed. 4754: A security-enabled universal group was created. 4755: A security-enabled universal group was changed. 4756: A member was added to a security-enabled universal group. 4757: A member was removed from a security-enabled universal group. 4758: A security-enabled universal group was deleted. 4764: A group's type was changed. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38034-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.2.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Security Group Management' is set to 'Success and Failure'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit Security Group Management>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports each event of security group management, such as when a security group is created, changed, or deleted or when a member is added to or removed from a security group. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of security group accounts. Events for this subcategory include: 4727: A security-enabled global group was created. 4728: A member was added to a security-enabled global group. 4729: A member was removed from a security-enabled global group. 4730: A security-enabled global group was deleted. 4731: A security-enabled local group was created. 4732: A member was added to a security-enabled local group. 4733: A member was removed from a security-enabled local group. 4734: A security-enabled local group was deleted. 4735: A security-enabled local group was changed. 4737: A security-enabled global group was changed. 4754: A security-enabled universal group was created. 4755: A security-enabled universal group was changed. 4756: A member was added to a security-enabled universal group. 4757: A member was removed from a security-enabled universal group. 4758: A security-enabled universal group was deleted. 4764: A group's type was changed. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38034-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.2.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Security State Change' is set to 'Success' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security State Change Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This subcategory reports changes in security state of the system, such as when the security subsystem starts and stops. Events for this subcategory include: 4608: Windows is starting up. 4609: Windows is shutting down. 4616: The system time was changed. 4621: Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38114-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.9.3

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Security State Change' is set to 'Success' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security State Change>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports changes in security state of the system, such as when the security subsystem starts and stops. Events for this subcategory include: 4608: Windows is starting up. 4609: Windows is shutting down. 4616: The system time was changed. 4621: Administrator recovered system from CrashOnAuditFail. Users who are not administrators will now be allowed to log on. Some auditable activity might not have been recorded. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-38114-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.9.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure'	Trivial

Vulnerability Details

This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include: 4610: An authentication package has been loaded by the Local Security Authority. 4611: A trusted logon process has been registered with the Local Security Authority. 4614: A notification package has been loaded by the Security Account Manager. 4622: A security package has been loaded by the Local Security Authority. 4697: A service was installed in the system. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36144-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.9.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Security System Extension' is set to 'Success and Failure'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit Security System Extension>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports the loading of extension code such as authentication packages by the security subsystem. Events for this subcategory include: 4610: An authentication package has been loaded by the Local Security Authority. 4611: A trusted logon process has been registered with the Local Security Authority. 4614: A notification package has been loaded by the Security Account Manager. 4622: A security package has been loaded by the Local Security Authority. 4697: A service was installed in the system. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36144-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.9.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

Trivial

Vulnerability Details

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights: Act as part of the operating system, Back up files and directories, Create a token object, Debug programs, Enable computer and user accounts to be trusted for delegation, Generate security audits, Impersonate a client after authentication, Load and unload device drivers, Manage auditing and security log, Modify firmware environment values, Replace a process-level token, Restore files and directories, and Take ownership of files or other objects. Auditing this subcategory will create a high volume of events. Events for this subcategory include: 4672: Special privileges assigned to new logon. 4673: A privileged service was called. 4674: An operation was attempted on a privileged object. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36267-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.8.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the

Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Sensitive Privilege Use' is set to 'Success and Failure'

Trivial

Vulnerability Details

This subcategory reports when a user account or service uses a sensitive privilege. A sensitive privilege includes the following user rights: Act as part of the operating system, Back up files and directories, Create a token object, Debug programs, Enable computer and user accounts to be trusted for delegation, Generate security audits, Impersonate a client after authentication, Load and unload device drivers, Manage auditing and security log, Modify firmware environment values, Replace a process-level token, Restore files and directories, and Take ownership of files or other objects. Auditing this subcategory will create a high volume of events. Events for this subcategory include: 4672: Special privileges assigned to new logon. 4673: A privileged service was called. 4674: An operation was attempted on a privileged object. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36267-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.8.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Privilege Use\Audit Sensitive Privilege Use>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log security audits Impact: If you enable this policy setting, the administrative burden can be significant, especially if you also configure the Retention method for the Security log to Do not overwrite events (clear log manually). This configuration causes a repudiation threat (a backup operator could deny that they backed up or restored data) to become a denial of service (DoS) vulnerability, because a server could be forced to shut down if it is overwhelmed with logon events and other security events that are written to the Security log. Also, because the shutdown is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. Although the NTFS file system guarantees its integrity when an ungraceful computer shutdown occurs, it cannot guarantee that every data file for every application will still be in a usable form when the computer restarts.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting determines whether the system shuts down if it is unable to log Security events. It is a requirement for Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certification to prevent auditable events from occurring if the audit system is unable to log them. Microsoft has chosen to meet this requirement by halting the system and displaying a stop message if the auditing system experiences a failure. When this policy setting is enabled, the system will be shut down if a security audit cannot be logged for any reason. If the Audit: Shut down system immediately if unable to log security audits setting is enabled, unplanned system failures can occur. Therefore, this policy setting is configured to Not Defined for both of the environments that are discussed in this chapter. The recommended state for this setting is: Disabled.

Rationale: If the computer is unable to record events to the Security log, critical evidence or important troubleshooting information may not be available for review after a security incident. Also, an attacker could potentially generate a large volume of Security log events to purposely force a computer shutdown.

CCE Reference Number: CCE-35907-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.2.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit: Shut down system immediately if unable to log security audits' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines whether the system shuts down if it is unable to log Security events. It is a requirement for Trusted Computer System Evaluation Criteria (TCSEC)-C2 and Common Criteria certification to prevent auditable events from occurring if the audit system is unable to log them. Microsoft has chosen to meet this requirement by halting the system and displaying a stop message if the auditing system experiences a failure. When this policy setting is enabled, the system will be shut down if a security audit cannot be logged for any reason. If the Audit: Shut down system immediately if unable to log security audits setting is enabled, unplanned system failures can occur. The administrative burden can be significant, especially if you also configure the Retention method for the Security log to Do not overwrite events (clear log manually). This configuration causes a repudiation threat (a backup operator could deny that they backed up or restored data) to become a denial of service (DoS) vulnerability, because a server could be forced to shut down if it is overwhelmed with logon events and other security events that are written to the Security log. Also, because the shutdown is not graceful, it is possible that irreparable damage to the operating system, applications, or data could result. Although the NTFS file system guarantees its integrity when an ungraceful computer shutdown occurs, it cannot guarantee that every data file for every application will still be in a usable form when the computer restarts. The recommended state for this setting is: Disabled.

Rationale: If the computer is unable to record events to the Security log, critical evidence or important troubleshooting information may not be available for review after a security incident. Also, an attacker could potentially generate a large volume of Security log events to purposely force a computer shutdown.

CCE Reference Number: CCE-35907-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.2.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Audit: Shut down system immediately if unable to log security audits>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Special Logon' is set to 'Success' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This subcategory reports when a special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level. Events for this subcategory include: 4964 : Special groups have been assigned to a new logon. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36266-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.5.5

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit Special Logon' is set to 'Success' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Logon/Logoff\Audit Special Logon>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This subcategory reports when a special logon is used. A special logon is a logon that has administrator-equivalent privileges and can be used to elevate a process to a higher level. Events for this subcategory include: 4964 : Special groups have been assigned to a new logon. The recommended state for this setting is: Success.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-36266-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.5.6

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit System Integrity Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports on violations of integrity of the security subsystem. Events for this subcategory include: 4612 : Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits. 4615: Invalid use of LPC port. 4618 : A monitored security event pattern has occurred. 4816: RPC detected an integrity violation while decrypting an incoming message. 5038 : Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error. 5056: A cryptographic self test was performed. 5057: A cryptographic primitive operation failed. 5060: Verification operation failed. 5061: Cryptographic operation. 5062: A kernel-mode cryptographic self test was performed. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37132-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.9.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit System Integrity' is set to 'Success and Failure' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\System\Audit System Integrity>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and

computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports on violations of integrity of the security subsystem. Events for this subcategory include: 4612 : Internal resources allocated for the queuing of audit messages have been exhausted, leading to the loss of some audits. 4615 : Invalid use of LPC port. 4618 : A monitored security event pattern has occurred. 4816 : RPC detected an integrity violation while decrypting an incoming message. 5038 : Code integrity determined that the image hash of a file is not valid. The file could be corrupt due to unauthorized modification or the invalid hash could indicate a potential disk device error. 5056: A cryptographic self test was performed. 5057: A cryptographic primitive operation failed. 5060: Verification operation failed. 5061: Cryptographic operation. 5062: A kernel-mode cryptographic self test was performed. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37132-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.9.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure: Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit User Account Management Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include: 4720: A user account was created. 4722: A user account was enabled. 4723: An attempt was made to change an account's password. 4724: An attempt was made to reset an account's password. 4725: A user account was disabled. 4726: A user account was deleted. 4738: A user account was changed. 4740: A user account was locked out. 4765: SID History was added to an account. 4766: An attempt to add SID History to an account failed. 4767: A user account was unlocked. 4780: The ACL was set on accounts which are members of administrators groups. 4781: The name of an account was changed: 4794: An attempt was made to set the Directory Services Restore Mode. 5376: Credential Manager credentials were backed up. 5377: Credential Manager credentials were restored from a backup. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37856-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 17.2.6

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Audit User Account Management' is set to 'Success and Failure' **Trivial**

Solution Details

To establish the recommended configuration via GP, set the following UI path to Success and Failure:

<Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Account Management\Audit User Account Management>

Impact: If no audit settings are configured, or if audit settings are too lax on the computers in your organization, security incidents might not be detected or not enough evidence will be available for network forensic analysis after security incidents occur. However, if audit settings are too severe, critically important entries in the Security log may be obscured by all of the meaningless entries and computer performance and the available amount of data storage may be seriously affected. Companies that operate in certain regulated industries may have legal obligations to log certain events or activities.

Vulnerability Details

This subcategory reports each event of user account management, such as when a user account is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. If you enable this Audit policy setting, administrators can track events to detect malicious, accidental, and authorized creation of user accounts. Events for this subcategory include: 4720: A user account was created. 4722: A user account was enabled. 4723: An attempt was made to change an account's password. 4724: An attempt was made to reset an account's password. 4725: A user account was disabled. 4726: A user account was deleted. 4738: A user account was changed. 4740: A user account was locked out. 4765: SID History was added to an account. 4766: An attempt to add SID History to an account failed. 4767: A user account was unlocked. 4780: The ACL was set on accounts which are members of administrators groups. 4781: The name of an account was changed: 4794: An attempt was made to set the Directory Services Restore Mode. 5376: Credential Manager credentials were backed up. 5377: Credential Manager credentials were restored from a backup. The recommended state for this setting is: Success and Failure.

Rationale: Auditing these events may be useful when investigating a security incident.

CCE Reference Number: CCE-37856-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 17.2.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Automatically send memory dumps for OS-generated error reports' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\Automatically send memory dumps for OS-generated error reports Impact: If you disable this policy setting, then all memory dumps are uploaded according to the default consent and notification settings.

Vulnerability Details

This policy setting controls whether memory dumps in support of OS-generated error reports can be sent to Microsoft automatically. This policy does not apply to error reports generated by 3rd-party products, or additional data other than memory dumps. The recommended state for this setting is: Disabled.

Rationale: Memory dumps may contain sensitive information and should not be automatically sent to anyone.

CCE Reference Number: CCE-36978-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.67.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Back up files and directories' is set to 'Administrators'

Trivial

Vulnerability Details

This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply. The recommended state for this setting is: Administrators.

Rationale: Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

CCE Reference Number: CCE-35912-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.8

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators. Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories Impact: Changes in the membership of the groups that have the Back up files and directories user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Back up files and directories' is set to 'Administrators'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators.

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Back up files and directories>

Impact: Changes in the membership of the groups that have the Back up files and directories user right could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that authorized backup administrators are still able to perform backup operations.

Vulnerability Details

This policy setting allows users to circumvent file and directory permissions to back up the system. This user right is enabled only when an application (such as NTBACKUP) attempts to access a file or directory through the NTFS file system backup application programming interface (API). Otherwise, the assigned file and directory permissions apply. The recommended state for this setting is: Administrators.

Rationale: Users who are able to back up data from a computer could take the backup media to a non-domain computer on which they have administrative privileges and restore the data. They could take ownership of the files and view any unencrypted data that is contained within the backup set.

CCE Reference Number: CCE-35912-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Block launching Windows Store apps with Windows Runtime API access from hosted content.' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\Block launching Windows Store apps with Windows Runtime API access from hosted content.>

Impact: Windows Store apps with Windows Runtime API access directly from web content cannot be launched (Windows Store apps without Windows Runtime API access from web content will not be affected).

Vulnerability Details

This policy setting controls whether Windows Store apps with Windows Runtime API access directly from web content can be launched. The recommended state for this setting is: Enabled.

Rationale: Blocking Apps from the web with direct access to the Windows API can prevent malicious apps from being run on a system. Only system administrators should be installing approved applications. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.6.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Block user from showing account details on sign-in' is set to 'Enabled' — Trivial

Vulnerability Details

This policy prevents the user from showing account details (email address or user name) on the sign-in screen. The recommended state for this setting is: Enabled.

Rationale: An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.25.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Enabled:

Computer Configuration\Policies\Administrative Templates\System\Logon\Block user from showing account details on sign-in

Note: This Group Policy path does not exist by default. An updated Group Policy template (Logon.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: The user cannot choose to show account details on the sign-in screen.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'	Trivial

Vulnerability Details

This policy setting allows you to specify which boot-start drivers are initialized based on a classification determined by an Early Launch Antimalware boot-start driver. The Early Launch Antimalware boot-start driver can return the following classifications for each boot-start driver: Good: The driver has been signed and has not been tampered with. Bad: The driver has been identified as malware. It is recommended that you do not allow known bad drivers to be initialized. Bad, but required for boot: The driver has been identified as malware, but the computer cannot successfully boot without loading this driver. Unknown: This driver has not been attested to by your malware detection application and has not been classified by the Early Launch Antimalware boot-start driver. If you enable this policy setting you will be able to choose which boot-start drivers to initialize the next time the computer is started. If you disable or do not configure this policy setting, the boot start drivers determined to be Good, Unknown or Bad but Boot Critical are initialized and the initialization of drivers determined to be Bad is skipped. If your malware detection application does not include an Early Launch Antimalware boot-start driver or if your Early Launch Antimalware boot-start driver has been disabled, this setting has no effect and all boot-start drivers are initialized. The recommended state for this setting is: Enabled: Good, unknown and bad but critical.

Rationale: This policy setting helps reduce the impact of malware that has already infected your system.

CCE Reference Number: CCE-37912-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.11.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Good, unknown and bad but critical: Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware\Boot-Start Driver Initialization Policy Impact: None - this is the default behavior.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Boot-Start Driver Initialization Policy' is set to 'Enabled: Good, unknown and bad but critical'

Trivial

Vulnerability Details

This policy setting allows you to specify which boot-start drivers are initialized based on a classification determined by an Early Launch Antimalware boot-start driver. The Early Launch Antimalware boot-start driver can return the following classifications for each boot-start driver:
Good: The driver has been signed and has not been tampered with.
Bad: The driver has been identified as malware. It is recommended that you do not allow known bad drivers to be initialized.
Bad, but required for boot: The driver has been identified as malware, but the computer cannot successfully boot without loading this driver.
Unknown: This driver has not been attested to by your malware detection application and has not been classified by the Early Launch Antimalware boot-start driver.

If you enable this policy setting you will be able to choose which boot-start drivers to initialize the next time the computer is started. If your malware detection application does not include an Early Launch Antimalware boot-start driver or if your Early Launch Antimalware boot-start driver has been disabled, this setting has no effect and all boot-start drivers are initialized. The recommended state for this setting is: Enabled: Good, unknown and bad but critical.

Rationale: This policy setting helps reduce the impact of malware that has already infected your system.

CCE Reference Number: CCE-37912-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.12.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Good, unknown and bad but critical:

<Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalware\Boot-Start Driver Initialization Policy>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'	**Trivial**

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time Impact: There should be no impact, because time synchronization for most organizations should be fully automated for all computers that belong to the domain. Computers that do not belong to the domain should be configured to synchronize with an external source.

Vulnerability Details

This policy setting determines which users and groups can change the time and date on the internal clock of the computers in your environment. Users who are assigned this user right can affect the appearance of event logs. When a computer's time setting is changed, logged events reflect the new time, not the actual time that the events occurred. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers.

Note: Discrepancies between the time on the local computer and on the domain controllers in your environment may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or obtain authorization to access domain resources after they are logged on. Also, problems will occur when Group Policy is applied to client computers if the system time is not synchronized with the domain controllers. The recommended state for this setting is: Administrators, LOCAL SERVICE.

Rationale: Users who can change the time on a computer could cause several problems. For example, time stamps on event log entries could be made inaccurate, time stamps on files and folders that are created or modified could be incorrect, and computers that belong to a domain may not be able to authenticate themselves or users who try to log on to the domain from them. Also, because the Kerberos authentication protocol requires that the requestor and authenticator have their clocks synchronized within an administrator-defined skew period, an attacker who changes a computer's time may cause that computer to be unable to obtain or grant Kerberos tickets.The risk from these types of events is mitigated on most domain controllers, member servers, and end-user computers because the Windows Time service automatically synchronizes time with domain controllers in the following ways:#x2022; All client desktop computers and member servers use the authenticating domain controller as their inbound time partner.#x2022; All domain controllers in a domain nominate the primary domain controller (PDC) emulator operations master as their inbound time partner.#x2022; All PDC emulator operations masters follow the hierarchy of domains in the selection of their inbound time partner.#x2022; The PDC emulator operations master at the root of the domain is authoritative for the organization. Therefore it is recommended that you configure this computer to synchronize with a reliable external time server.This vulnerability becomes much more serious if an attacker is able to change the system time and then stop the Windows Time service or reconfigure it to synchronize with a time server that is not accurate.

CCE Reference Number: CCE-37452-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Change the system time' is set to 'Administrators, LOCAL SERVICE'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the system time>

Impact: There should be no impact, because time synchronization for most organizations should be fully automated for all computers that belong to the domain. Computers that do not belong to the domain should be configured to synchronize with an external source.

Vulnerability Details

This policy setting determines which users and groups can change the time and date on the internal clock of the computers in your environment. Users who are assigned this user right can affect the appearance of event logs. When a computer's time setting is changed, logged events reflect the new time, not the actual time that the events occurred. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers. Note: Discrepancies between the time on the local computer and on the domain controllers in your environment may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or obtain authorization to access domain resources after they are logged on. Also, problems will occur when Group Policy is applied to client computers if the system time is not synchronized with the domain controllers. The recommended state for this setting is: Administrators, LOCAL SERVICE.

Rationale: Users who can change the time on a computer could cause several problems. For example, time stamps on event log entries could be made inaccurate, time stamps on files and folders that are created or modified could be incorrect, and computers that belong to a domain may not be able to authenticate themselves or users who try to log on to the domain from them. Also, because the Kerberos authentication protocol requires that the requestor and authenticator have their clocks synchronized within an administrator-defined skew period, an attacker who changes a computer's time may cause that computer to be unable to obtain or grant Kerberos tickets. The risk from these types of events is mitigated on most domain controllers, member servers, and end-user computers because the Windows Time service automatically synchronizes time with domain controllers in the following ways: All client desktop computers and member servers use the authenticating domain controller as their inbound time partner. All domain controllers in a domain nominate the primary domain controller (PDC) emulator operations master as their inbound time partner. All PDC emulator operations masters follow the hierarchy of domains in the selection of their inbound time partner. The PDC emulator operations master at the root of the domain is authoritative for the organization. Therefore it is recommended that you configure this computer to synchronize with a reliable external time server. This vulnerability becomes much more serious if an attacker is able to change the system time and then stop the Windows Time service or reconfigure it to synchronize with a time server that is not accurate.

CCE Reference Number: CCE-37452-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE' — Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the time zone Impact: None. This is the default configuration.

Vulnerability Details

This setting determines which users can change the time zone of the computer. This ability holds no great danger for the computer and may be useful for mobile workers. The recommended state for this setting is: Administrators, LOCAL SERVICE.

Rationale: Changing the time zone represents little vulnerability because the system time is not affected. This setting merely enables users to display their preferred time zone while being synchronized with domain controllers in different time zones.

CCE Reference Number: CCE-37700-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.10

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Change the time zone' is set to 'Administrators, LOCAL SERVICE'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Change the time zone>

Impact: None - this is the default configuration.

Vulnerability Details

This setting determines which users can change the time zone of the computer. This ability holds no great danger for the computer and may be useful for mobile workers. The recommended state for this setting is: Administrators, LOCAL SERVICE.

Rationale: Changing the time zone represents little vulnerability because the system time is not affected. This setting merely enables users to display their preferred time zone while being synchronized with domain controllers in different time zones.

CCE Reference Number: CCE-37700-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configuration of wireless settings using Windows Connect Now' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Network\Windows Connect Now\Configuration of wireless settings using Windows Connect Now>

Impact: WCN operations are disabled over all media.

Vulnerability Details

This policy setting allows the configuration of wireless settings using Windows Connect Now (WCN). The WCN Registrar enables the discovery and configuration of devices over Ethernet (UPnP) over In-band 802.11 Wi-Fi through the Windows Portable Device API (WPD) and via USB Flash drives. Additional options are available to allow discovery and configuration over a specific medium. The recommended state for this setting is: Disabled.

Rationale: This setting enhances the security of the environment and reduces the overall risk exposure related to user configuration of wireless settings.

CCE Reference Number: CCE-37481-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.20.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' Trivial

Vulnerability Details

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work:- Notify before downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: Enabled.

Rationale: Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

CCE Reference Number: CCE-36172-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.85.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Automatic Updates' is set to 'Enabled' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows

Update\Configure Automatic Updates>

Impact: Critical operating system updates and service packs will be installed as necessary.

Vulnerability Details

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic Updates Properties dialog box to specify how the service will work: - Notify before downloading any updates and notify again before installing them. - Download the updates automatically and notify when they are ready to be installed. (Default setting) - Automatically download updates and install them on the schedule specified below. The recommended state for this setting is: Enabled.

Note: The sub-setting "Configure automatic updating:" has 4 possible values all of them are valid depending on organizational needs, however if feasible we suggest using a value of 4 - Auto download and schedule the install. This suggestion is not a scored requirement.

Rationale: Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

CCE Reference Number: CCE-36172-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.90.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day'

Trivial

Vulnerability Details

This policy setting specifies whether computers in your environment will receive security updates from Windows Update or WSUS. If you configure this policy setting to Enabled, the operating system will recognize when a network connection is available and then use the network connection to search Windows Update or your designated intranet site for updates that apply to them. After you configure this policy setting to Enabled, select one of the following three options in the Configure Automatic

Updates Properties dialog box to specify how the service will work:- Notify before downloading any updates and notify again before installing them.- Download the updates automatically and notify when they are ready to be installed. (Default setting)- Automatically download updates and install them on the schedule specified below. If you disable this policy setting, you will need to download and manually install any available updates from Windows Update. The recommended state for this setting is: 0 - Every day.

Rationale: Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

CCE Reference Number: CCE-36172-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.85.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to 0 - Every day: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day Impact: Critical operating system updates and service packs will automatically download and install at 3:00 A.M. daily.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Automatic Updates: Scheduled install day' is set to '0 - Every day' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 0 - Every day:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Configure Automatic Updates: Scheduled install day>

Impact: If 4 - Auto download and schedule the install is selected in 18.9.85.1, critical operating system updates and service packs will automatically download every day (at 3:00 A.M., by default).

Vulnerability Details

This policy setting specifies when computers in your environment will receive security updates from Windows Update or WSUS. The recommended state for this setting is: 0 - Every day.

Note: This setting is only applicable if 4 - Auto download and schedule the install is selected in 18.9.85.1. It will have no impact if any other option is selected.

Rationale: Although each version of Windows is thoroughly tested before release, it is possible that problems will be discovered after the products are shipped. The Configure Automatic Updates setting can help you ensure that the computers in your environment will always have the most recent critical operating system updates and service packs installed.

CCE Reference Number: CCE-36172-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.90.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure cookies' is set to 'Enabled: Block only 3rd-party cookies' or higher

Trivial

Vulnerability Details

This setting lets you configure how your company deals with cookies. The recommended state for this setting is: Enabled: Block only 3rd-party cookies. Configuring this setting to Enabled: Block all cookies also conforms with the benchmark.

Rationale: Cookies can pose a serious privacy concern, although many websites depend on them for operation. It is recommended when possible to block 3rd party cookies in order to reduce tracking.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Block only 3rd-party cookies(or, if applicable for your environment, Enabled: Block all cookies):

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure cookies>

Impact: If you select "Block only 3rd-party cookies", cookies from 3rd-party websites will be blocked, but 1st-party website cookies will still be permitted. If you select "Block all cookies", cookies from all websites will be blocked.

Note: Blocking all cookies may interfere with functionality on some websites that depend on them for session tracking and/or login credentials.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Default consent' is set to 'Enabled: Always ask before sending data'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Always ask before sending data: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\Consent\Configure Default consent Impact: By setting to always ask before sending data: Windows prompts users for consent to send reports.

Vulnerability Details

This setting allows you to set the default consent handling for error reports. The recommended state for this setting is: Enabled: Always ask before sending data

Rationale: Error reports may contain sensitive information and should not be sent to anyone automatically.

CCE Reference Number: CCE-37112-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.67.2.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance Impact: Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests.

Vulnerability Details

This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer. If you enable this policy setting, users on this computer can get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you disable this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you do not configure this policy setting, users on this computer cannot get help from their corporate technical support staff using Offer (Unsolicited) Remote Assistance. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." When you configure this policy setting, you also specify the list of users or user groups that are allowed to offer remote assistance. To configure the list of helpers, click "Show." In the window that opens, you can enter the names of the helpers. Add each user or group one by one. When you enter the name of the helper user or user groups, use the following format:<Domain Name>\<User Name> or<Domain Name>\<Group Name> If you enable this policy setting, you should also enable firewall exceptions to allow Remote Assistance communications. The firewall exceptions required for Offer (Unsolicited) Remote Assistance depend on the version of Windows you are running: Windows Vista and later:Enable the Remote Assistance exception for the domain profile.

The exception must contain:Port 135:TCP%WINDIR%\System32\msra.exe%WINDIR%\System32\raserver.exe Windows XP with Service Pack 2 (SP2) and Windows XP Professional x64 Edition with Service Pack 1 (SP1):Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\He
For computers running Windows Server 2003 with Service Pack 1 (SP1)Port 135:TCP%WINDIR%\PCHealth\HelpCtr\Binaries\Helpsvc.exe%WINDIR%\PCHealth\HelpCtr\Binaries\He
Remote Desktop Exception The recommended state for this setting is: Disabled.

Rationale: A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

CCE Reference Number: CCE-36388-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.30.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Offer Remote Assistance' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Offer Remote Assistance>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows you to turn on or turn off Offer (Unsolicited) Remote Assistance on this computer. Help desk and support personnel will not be able to proactively offer assistance, although they can still respond to user assistance requests. The recommended state for this setting is: Disabled.

Rationale: A user might be tricked and accept an unsolicited Remote Assistance offer from a malicious user.

CCE Reference Number: CCE-36388-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.31.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Password Manager' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure Password Manager>

Impact: Employees will not be able to use Password Manager.

Vulnerability Details

This setting lets you decide whether employees can save their passwords locally, using Password

Manager. The recommended state for this setting is: Disabled.

Rationale: Using Password Manager can potentially makes it easier for an unauthorized user who gains access to the users desktop (including a coworker who sits down at a users desk soon after the user walks away and forgets to lock their workstation), to log in to sites as the user, without needing to know or enter the password. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Pop-up Blocker' is set to 'Enabled' Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure Pop-up Blocker>

Impact: None - this is the default configuration.

Vulnerability Details

This setting lets you decide whether to turn on Pop-up Blocker and whether to allow pop-ups to appear in secondary windows. The recommended state for this setting is: Enabled.

Rationale: The Pop-up Blocker serves an important purpose by blocking malicious popups and helping prevent the machine from being compromised. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.5

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Do not apply during periodic background processing option to FALSE (unchecked): Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Vulnerability Details

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart. The recommended state for this setting is: Enabled: FALSE (unchecked).

Rationale: Setting this option to false (unchecked) will ensure that domain policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

CCE Reference Number: CCE-36169-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.18.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure registry policy processing: Do not apply during periodic background processing' is set to 'Enabled: FALSE'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Do not apply during periodic background processing option to FALSE (unchecked):

<Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing>

Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Vulnerability Details

The "Do not apply during periodic background processing" option prevents the system from updating affected policies in the background while the computer is in use. When background updates are disabled, policy changes will not take effect until the next user logon or system restart. The recommended state for this setting is: Enabled: FALSE (unchecked).

Rationale: Setting this option to false (unchecked) will ensure that domain policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

CCE Reference Number: CCE-36169-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.19.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Process even if the Group Policy objects have not changed option to TRUE (checked): Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing Impact: Group Policies will be reapplied every time they are refreshed, which could have a slight impact on performance.

Vulnerability Details

The "Process even if the Group Policy objects have not changed" option updates and reapplies policies even if the policies have not changed. The recommended state for this setting is: Enabled: TRUE (checked).

Rationale: Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

CCE Reference Number: CCE-36169-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.18.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure registry policy processing: Process even if the Group Policy objects have not changed' is set to 'Enabled: TRUE'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, then set the Process even if the Group Policy objects have not changed option to TRUE (checked):

<Computer Configuration\Policies\Administrative Templates\System\Group Policy\Configure registry policy processing>

Impact: Group Policies will be reapplied even if they have not been changed, which could have a slight impact on performance.

Vulnerability Details

The "Process even if the Group Policy objects have not changed" option updates and reapplies policies even if the policies have not changed. The recommended state for this setting is: Enabled: TRUE (checked).

Rationale: Setting this option to true (checked) will ensure unauthorized changes that might have been configured locally are forced to match the domain-based Group Policy settings again.

CCE Reference Number: CCE-36169-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.19.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure search suggestions in Address bar' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure search suggestions in Address bar>

Impact: Employees will not see search suggestions in the Address bar of Microsoft Edge.

Vulnerability Details

This setting lets you decide whether search suggestions should appear in the Address bar of Microsoft Edge. The recommended state for this setting is: Disabled.

Rationale: Having search suggestions sent out to be processed is considered a privacy concern. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure SmartScreen Filter' is set to 'Enabled' — Trivial

Vulnerability Details

This setting lets you decide whether to turn on SmartScreen Filter. SmartScreen Filter provides warning messages to help protect your employees from potential phishing scams and malicious software. The recommended state for this setting is: Enabled.

Rationale: SmartScreen serves an important purpose as it helps to warn users of possible malicious sites and files. Allowing users to turn off this setting can make the browser become more vulnerable to compromise. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.7

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Configure SmartScreen Filter>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' — Trivial

Vulnerability Details

This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer. If you enable this policy setting, users on this computer can use email or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings. If you disable this policy setting, users on this computer cannot use email or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer. If you do not configure this policy setting, users can turn on or turn off Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings. If you enable this policy setting, you have two ways to allow helpers to provide Remote Assistance: "Allow helpers to only view the computer" or "Allow helpers to remotely control the computer." The "Maximum ticket time" policy setting sets a limit on the amount of time that a Remote Assistance invitation created by using email or file transfer can remain open. The "Select the method for sending email invitations" setting specifies which email standard to use to send Remote Assistance invitations. Depending on your email program, you can use either the Mailto standard (the invitation recipient connects through an Internet link) or the SMAPI (Simple MAPI) standard (the invitation is attached to your email message). This policy setting is not available in Windows Vista since SMAPI is the only method supported. If you enable this policy setting you should also enable appropriate firewall exceptions to allow Remote Assistance communications. The recommended state for this setting is: Disabled.

Rationale: There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user's computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

CCE Reference Number: CCE-37281-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.30.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance Impact: If you enable this policy, users on this computer can use email or file transfer to ask someone for help. Also, users can use instant messaging programs to allow connections to this computer, and you can configure additional Remote Assistance settings. If you disable this policy, users on this computer cannot use email or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer. If you don't configure this policy, users can enable or disable Solicited (Ask for) Remote Assistance themselves in System Properties in Control Panel. Users can also configure Remote Assistance settings.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Solicited Remote Assistance' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\System\Remote Assistance\Configure Solicited Remote Assistance>

Impact: Users on this computer cannot use e-mail or file transfer to ask someone for help. Also, users cannot use instant messaging programs to allow connections to this computer.

Vulnerability Details

This policy setting allows you to turn on or turn off Solicited (Ask for) Remote Assistance on this computer. The recommended state for this setting is: Disabled.

Rationale: There is slight risk that a rogue administrator will gain access to another user's desktop session, however, they cannot connect to a user's computer unannounced or control it without permission from the user. When an expert tries to connect, the user can still choose to deny the connection or give the expert view-only privileges. The user must explicitly click the Yes button to allow the expert to remotely control the workstation.

CCE Reference Number: CCE-37281-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.31.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Configure Watson events' is set to 'Disabled' — Trivial

Vulnerability Details

This policy setting allows you to configure whether or not Watson events are sent. The recommended state for this setting is: Disabled.

Rationale: Watson events are the reports that get sent to Microsoft when a program or service crashes or fails, including the possibility of automatic submission. Preventing this information from being sent can help reduce privacy concerns.

CCE Reference Number: CCE-36950-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.69.8.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender\Reporting\Configure Watson events

Note: This Group Policy path does not exist by default. An updated Group Policy template (WindowsDefender.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: Watson events will not be sent to Microsoft automatically when a program or service crashes or fails.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled' — Trivial

Vulnerability Details

This policy setting allows you to manage the behavior of Windows SmartScreen. Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled. The recommended state for this setting is: Enabled.

Rationale: Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. However, due to the fact that some information is sent to Microsoft about files and programs run on PCs some organizations may prefer to disable it.

CCE Reference Number: CCE-35859-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.30.2

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Configure Windows SmartScreen>

Impact: Only administrators will be able to run unrecognized programs downloaded from the Internet. If users with a standard account try, they won't be able to unless they get an administrator to authorize it.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Configure Windows SmartScreen' is set to 'Enabled: Require approval from an administrator before running downloaded unknown software' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: Require approval from an administrator before running downloaded unknown software: Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Configure Windows SmartScreen Impact: Only administrators will be able to run unrecognized programs downloaded from the Internet. If users with a standard account try, they won't be able to unless they get an administrator to authorize it.

Vulnerability Details

This policy setting allows you to manage the behavior of Windows SmartScreen. Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. Some information is sent to Microsoft about files and programs run on PCs with this feature enabled. If you enable this policy setting, Windows SmartScreen behavior may be controlled by setting one of the following options: Require approval from an administrator before running downloaded unknown software Give user a warning before running downloaded unknown software Turn off SmartScreen If you disable or do not configure this policy setting, Windows SmartScreen behavior is managed by administrators on the PC by using Windows SmartScreen Settings in Action Center. The recommended state for this setting is: Enabled: Require approval from an administrator before running downloaded unknown software.

Rationale: Windows SmartScreen helps keep PCs safer by warning users before running unrecognized programs downloaded from the Internet. However, due to the fact that some information is sent to Microsoft about files and programs run on PCs some organizations may prefer to disable it.

CCE Reference Number: CCE-35859-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.28.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Continue experiences on this device' is set to 'Disabled'

Trivial

Vulnerability Details

This policy setting determines whether the Windows device is allowed to participate in cross-device experiences (continue experiences). The recommended state for this setting is: Disabled.

Rationale: A cross-device experience is when a system can access app and send messages to other

devices. In an enterprise environment only trusted systems should be communicating within the network. Access to any other system should be prohibited.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.19.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\System\Group Policy\Continue experiences on this device>

Impact: The Windows device will not be discoverable by other devices, and cannot participate in cross-device experiences.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile Impact: None. This is the default configuration.

Vulnerability Details

This policy setting allows users to change the size of the pagefile. By making the pagefile extremely large or extremely small, an attacker could easily affect the performance of a compromised computer. The recommended state for this setting is: Administrators.

Rationale: Users who can change the page file size could make it extremely small or move the file to a highly fragmented storage volume, which could cause reduced computer performance.

CCE Reference Number: CCE-35821-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.11

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Create a pagefile' is set to 'Administrators' — Trivial

Vulnerability Details

This policy setting allows users to change the size of the pagefile. By making the pagefile extremely large or extremely small, an attacker could easily affect the performance of a compromised computer. The recommended state for this setting is: Administrators.

Rationale: Users who can change the page file size could make it extremely small or move the file to a highly fragmented storage volume, which could cause reduced computer performance.

CCE Reference Number: CCE-35821-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.11

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a pagefile>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Create a token object' is set to 'No One' — Trivial

Vulnerability Details

This policy setting allows a process to create an access token, which may provide elevated rights to access sensitive data. The recommended state for this setting is: No One.

Rationale: A user account that is given this user right has complete control over the system and can lead to the system being compromised. It is highly recommended that you do not assign any user accounts this right. The operating system examines a user's access token to determine the level of the user's privileges. Access tokens are built when users log on to the local computer or connect to a remote computer over a network. When you revoke a privilege, the change is immediately recorded, but the change is not reflected in the user's access token until the next time the user logs on or connects. Users with the ability to create or modify tokens can change the level of access for any currently logged on account. They could escalate their own privileges or create a DoS condition.

CCE Reference Number: CCE-36861-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.12

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a token object Impact: None. This is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Create a token object' is set to 'No One' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create a token object>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows a process to create an access token, which may provide elevated rights to access sensitive data. The recommended state for this setting is: No One.

Rationale: A user account that is given this user right has complete control over the system and can lead to the system being compromised. It is highly recommended that you do not assign any user accounts this right. The operating system examines a user's access token to determine the level of the user's privileges. Access tokens are built when users log on to the local computer or connect to a remote computer over a network. When you revoke a privilege, the change is immediately recorded, but the change is not reflected in the user's access token until the next time the user logs on or connects. Users with the ability to create or modify tokens can change the level of access for any currently logged on account. They could escalate their own privileges or create a DoS condition.

CCE Reference Number: CCE-36861-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.12

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE'

Trivial

Vulnerability Details

This policy setting determines whether users can create global objects that are available to all sessions. Users can still create objects that are specific to their own session if they do not have this user right. Users who can create global objects could affect processes that run under other users' sessions. This capability could lead to a variety of problems, such as application failure or data corruption. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

Rationale: Users who can create global objects could affect Windows services and processes that run under other user or system accounts. This capability could lead to a variety of problems, such as application failure, data corruption and elevation of privilege.

CCE Reference Number: CCE-37453-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.13

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create global objects Impact: None. This is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Create global objects' is set to 'Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE' Trivial

Vulnerability Details

This policy setting determines whether users can create global objects that are available to all sessions. Users can still create objects that are specific to their own session if they do not have this user right. Users who can create global objects could affect processes that run under other users' sessions. This capability could lead to a variety of problems, such as application failure or data corruption. The recommended state for this setting is: Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE.

Note: A Member Server with Microsoft SQL Server and its optional "Integration Services" component installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale: Users who can create global objects could affect Windows services and processes that run under other user or system accounts. This capability could lead to a variety of problems, such as application failure, data corruption and elevation of privilege.

CCE Reference Number: CCE-37453-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.13

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, LOCAL SERVICE, NETWORK SERVICE, SERVICE:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create global objects>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create permanent shared objects Impact: None. This is the default configuration.

Vulnerability Details

This user right is useful to kernel-mode components that extend the object namespace. However, components that run in kernel mode have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right. The recommended state for this setting is: No One.

Rationale: Users who have the Create permanent shared objects user right could create new shared objects and expose sensitive data to the network.

CCE Reference Number: CCE-36532-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.14

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Create permanent shared objects' is set to 'No One' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Create permanent shared objects>

Impact: None - this is the default configuration.

Vulnerability Details

This user right is useful to kernel-mode components that extend the object namespace. However, components that run in kernel mode have this user right inherently. Therefore, it is typically not necessary to specifically assign this user right. The recommended state for this setting is: No One.

Rationale: Users who have the Create permanent shared objects user right could create new shared objects and expose sensitive data to the network.

CCE Reference Number: CCE-36532-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.14

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Debug programs' is set to 'Administrators' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs Impact: If you revoke this user right, no one will be able to debug programs. However, typical circumstances rarely require this capability on production computers. If a problem arises that requires an application to be debugged on a production server, you can move the server to a different OU temporarily and assign the Debug programs user right to a separate Group Policy for that OU. The service account that is used for the cluster service needs the Debug programs privilege; if it does not have it, Windows Clustering will fail. For additional information about how to configure Windows Clustering in conjunction with computer hardening, see Microsoft Knowledge Base article 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server. Tools that are used to manage processes will be unable to affect processes that are not owned by the person who runs the tools. For example, the Windows Server 2003 Resource Kit tool Kill.exe requires this user right for administrators to terminate processes that they did not start.

Vulnerability Details

This policy setting determines which user accounts will have the right to attach a debugger to any process or to the kernel, which provides complete access to sensitive and critical operating system components. Developers who are debugging their own applications do not need to be assigned this user right; however, developers who are debugging new system components will need it. The recommended state for this setting is: Administrators.

Rationale: The Debug programs user right can be exploited to capture sensitive computer information from system memory, or to access and modify kernel or application structures. Some attack tools exploit this user right to extract hashed passwords and other private security information, or to insert rootkit code. By default, the Debug programs user right is assigned only to administrators, which helps to mitigate the risk from this vulnerability.

CCE Reference Number: CCE-37075-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.16

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Debug programs' is set to 'Administrators' — Trivial

Vulnerability Details

This policy setting determines which user accounts will have the right to attach a debugger to any process or to the kernel, which provides complete access to sensitive and critical operating system components. Developers who are debugging their own applications do not need to be assigned this user right; however, developers who are debugging new system components will need it. The recommended state for this setting is: Administrators.

Rationale: The Debug programs user right can be exploited to capture sensitive computer information from system memory, or to access and modify kernel or application structures. Some attack tools exploit this user right to extract hashed passwords and other private security information, or to insert rootkit code. By default, the Debug programs user right is assigned only to administrators, which helps to mitigate the risk from this vulnerability.

CCE Reference Number: CCE-37075-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.16

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Debug programs>

Impact: If you revoke this user right, no one will be able to debug programs. However, typical circumstances rarely require this capability on production computers. If a problem arises that requires an application to be debugged on a production server, you can move the server to a different OU temporarily and assign the Debug programs user right to a separate Group Policy for that OU. The service account that is used for the cluster service needs the Debug programs privilege; if it does not have it, Windows Clustering will fail. For additional information about how to configure Windows Clustering in conjunction with computer hardening, see Microsoft Knowledge Base article 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server. Tools that are used to manage processes will be unable to affect processes that are not owned by the person who runs the tools. For example, the Windows Server 2003 Resource Kit tool Kill.exe requires this user right for administrators to terminate processes that they did not start.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Default Action and Mitigation Settings' is set to 'Enabled' (plus subsettings)	Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Action and Mitigation Settings Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Vulnerability Details

This setting configures the default action after detection and advanced ROP mitigation. The recommended state for this setting is: Default Action and Mitigation Settings - Enabled Deep Hooks - Enabled Anti Detours - Enabled Banned Functions - Enabled Exploit Action - User Configured

Rationale: These advanced mitigations for ROP mitigations apply to all configured software in EMET. Deep Hooks protects critical APIs and the subsequent lower level APIs used by the top level critical API. Anti Detours renders ineffective exploits that evade hooks by executing a copy of the hooked function prologue and then jump to the function past the prologue. Banned Functions will block calls to ntdll!LdrHotPatchRoutine to mitigate potential exploits abusing the API.

CCE Reference Number: CCE-38427-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.22.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Default Protections for Internet Explorer' is set to 'Enabled'	Trivial

Vulnerability Details

This settings determine if EMET mitigations are applied to Internet Explorer. The recommended state for this setting is: Enabled.

Rationale: Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it.

CCE Reference Number: CCE-36570-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.22.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Internet Explorer

Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Default Protections for Popular Software' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Popular Explorer Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Vulnerability Details

This settings determine if EMET mitigations are applied to other popular software. The recommended state for this setting is: Enabled.

Rationale: Applying EMET mitigations to popular software packages will help reduce the reliability of exploits that target them. CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.22.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Default Protections for Recommended Software' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\Default Protections for Recommended Software

Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Vulnerability Details

This settings determine if recommended EMET mitigations are applied to WordPad, applications that are part of the Microsoft Office suite, Adobe Acrobat, Adobe Reader, and Oracle Java. The recommended state for this setting is: Enabled.

Rationale: Applying EMET mitigations to Internet Explorer will help reduce the reliability of exploits that target it. CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.22.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job Impact: If you assign the Deny log on as a batch job user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely. For example, if you assign this user right to the IWAM_<ComputerName> account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the Guests group, but on a computer that was upgraded from Windows 2000 this account is a member of the Guests group. Therefore, it is important that you understand which accounts belong to any groups that you assign the Deny log on as a batch job user right.

Vulnerability Details

This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right. The Deny log on as a batch job user right overrides the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk. The recommended state for this setting is to include: Guests.

Rationale: Accounts that have the Deny log on as a batch job user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

CCE Reference Number: CCE-36923-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.18

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Deny log on as a batch job' to include 'Guests' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to include Guests:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a batch job>

Impact: If you assign the Deny log on as a batch job user right to other accounts, you could deny users who are assigned to specific administrative roles the ability to perform their required job activities. You should confirm that delegated tasks will not be affected adversely. For example, if you assign this user right to the IWAM_(ComputerName) account, the MSM Management Point will fail. On a newly installed computer that runs Windows Server 2003 this account does not belong to the Guests group, but on a computer that was upgraded from Windows 2000 this account is a member of the Guests group. Therefore, it is important that you understand which accounts belong to any groups that you assign the Deny log on as a batch job user right.

Vulnerability Details

This policy setting determines which accounts will not be able to log on to the computer as a batch job. A batch job is not a batch (.bat) file, but rather a batch-queue facility. Accounts that use the Task Scheduler to schedule jobs need this user right. The Deny log on as a batch job user right overrides the Log on as a batch job user right, which could be used to allow accounts to schedule jobs that consume excessive system resources. Such an occurrence could cause a DoS condition. Failure to assign this user right to the recommended accounts can be a security risk. The recommended state for this setting is to include: Guests.

Rationale: Accounts that have the Deny log on as a batch job user right could be used to schedule jobs that could consume excessive computer resources and cause a DoS condition.

CCE Reference Number: CCE-36923-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.18

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Deny log on as a service' to include 'Guests' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service Impact: If you assign the Deny log on as a service user right to specific accounts, services may not be able to start and a DoS condition could result.

Vulnerability Details

This security setting determines which service accounts are prevented from registering a process as a service. This policy setting supersedes the Log on as a service policy setting if an account is subject to both policies. The recommended state for this setting is to include: Guests.

Note: This security setting does not apply to the System, Local Service, or Network Service accounts.

Rationale: Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the System account.

CCE Reference Number: CCE-36877-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.19

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Deny log on as a service' to include 'Guests' Trivial

Vulnerability Details

This security setting determines which service accounts are prevented from registering a process as a service. This policy setting supersedes the Log on as a service policy setting if an account is subject to both policies. The recommended state for this setting is to include: Guests.

Note: This security setting does not apply to the System, Local Service, or Network Service accounts.

Rationale: Accounts that can log on as a service could be used to configure and start new unauthorized services, such as a keylogger or other malicious software. The benefit of the specified countermeasure is somewhat reduced by the fact that only users with administrative privileges can install and configure services, and an attacker who has already attained that level of access could configure the service to run with the System account.

CCE Reference Number: CCE-36877-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.19

Solution Details

To establish the recommended configuration via GP, set the following UI path to include Guests:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on as a service>

Impact: If you assign the Deny log on as a service user right to specific accounts, services may not be able to start and a DoS condition could result.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Deny log on locally' to include 'Guests' — Trivial

Vulnerability Details

This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies. Important: If you apply this security policy to the Everyone group, no one will be able to log on locally. The recommended state for this setting is to include: Guests.

Rationale: Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

CCE Reference Number: CCE-37146-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.20

Solution Details

To establish the recommended configuration via GP, set the following UI path to include Guests: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally Impact: If you assign the Deny log on locally user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the ASPNET account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Deny log on locally' to include 'Guests' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to include Guests:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on locally>

Impact: If you assign the Deny log on locally user right to additional accounts, you could limit the abilities of users who are assigned to specific roles in your environment. However, this user right should explicitly be assigned to the ASPNET account on computers that run IIS 6.0. You should confirm that delegated activities will not be adversely affected.

Vulnerability Details

This security setting determines which users are prevented from logging on at the computer. This policy setting supersedes the Allow log on locally policy setting if an account is subject to both policies.

Important: If you apply this security policy to the Everyone group, no one will be able to log on locally. The recommended state for this setting is to include: Guests.

Rationale: Any account with the ability to log on locally could be used to log on at the console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

CCE Reference Number: CCE-37146-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.20

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'

Trivial

Vulnerability Details

This policy setting determines whether users can log on as Terminal Services clients. After the baseline member server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. The recommended state for this setting is to include: Guests, Local account.

Caution: Configuring a standalone (non-domain-joined) server as described above may result in an inability to remotely administer the server.

Rationale: Any account with the right to log on through Terminal Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

CCE Reference Number: CCE-36867-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.21

Solution Details

To establish the recommended configuration via GP, set the following UI path to include Guests, Local account: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services Impact: If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Deny log on through Remote Desktop Services' to include 'Guests, Local account'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to include Guests, Local account:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Deny log on through Remote Desktop Services>

Impact: If you assign the Deny log on through Terminal Services user right to other groups, you could limit the abilities of users who are assigned to specific administrative roles in your environment. Accounts that have this user right will be unable to connect to the computer through either Terminal Services or Remote Assistance. You should confirm that delegated tasks will not be negatively impacted.

Vulnerability Details

This policy setting determines whether users can log on as Terminal Services clients. After the baseline member server is joined to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end-user processing. The recommended state for this setting is to include: Guests, Local account. Caution: Configuring a standalone (non-domain-joined) server as described above may result in an inability to remotely administer the server.

Rationale: Any account with the right to log on through Terminal Services could be used to log on to the remote console of the computer. If this user right is not restricted to legitimate users who need to log on to the console of the computer, unauthorized users might download and run malicious software that elevates their privileges.

CCE Reference Number: CCE-36867-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.21

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media Impact: None - this is the default value. Only Administrators will be able to format and eject removable NTFS media.

Vulnerability Details

This policy setting determines who is allowed to format and eject removable NTFS media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges. The recommended state for this setting is: Administrators.

Rationale: Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

CCE Reference Number: CCE-37701-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.4.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Devices: Allowed to format and eject removable media' is set to 'Administrators' — Trivial

Vulnerability Details

This policy setting determines who is allowed to format and eject removable NTFS media. You can use this policy setting to prevent unauthorized users from removing data on one computer to access it on another computer on which they have local administrator privileges. The recommended state for this setting is: Administrators.

Rationale: Users may be able to move data on removable disks to a different computer where they have administrative privileges. The user could then take ownership of any file, grant themselves full control, and view or modify any file. The fact that most removable storage devices will eject media by pressing a mechanical button diminishes the advantage of this policy setting.

CCE Reference Number: CCE-37701-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.4.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Allowed to format and eject removable media>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'

Trivial

Vulnerability Details

For a computer to print to a shared printer, the driver for that shared printer must be installed on the local computer. This security setting determines who is allowed to install a printer driver as part of connecting to a shared printer. If this setting is enabled, only Administrators can install a printer driver as part of connecting to a shared printer. If this setting is disabled, any user can install a printer driver as part of connecting to a shared printer. The recommended state for this setting is: Enabled.

Note: This setting does not affect the ability to add a local printer. This setting does not affect Administrators.

Rationale: It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, you should allow only Administrators, not users, to do so on servers, because printer driver installation on a server may unintentionally cause the computer to become less stable. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious software that masquerades as a printer driver. It is feasible for an attacker to disguise a Trojan horse program as a printer driver. The program may appear to users as if they must use it to print, but such a program could unleash malicious code on your computer network.

CCE Reference Number: CCE-37942-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.4.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers Impact: Only Administrators will be able to install a printer driver as part of connecting to a shared printer. The ability to add a local printer will not be affected.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Devices: Prevent users from installing printer drivers' is set to 'Enabled'

Trivial

Vulnerability Details

For a computer to print to a shared printer, the driver for that shared printer must be installed on the local computer. This security setting determines who is allowed to install a printer driver as part of connecting to a shared printer. The recommended state for this setting is: Enabled.

Note: This setting does not affect the ability to add a local printer. This setting does not affect Administrators.

Rationale: It may be appropriate in some organizations to allow users to install printer drivers on their own workstations. However, you should allow only Administrators, not users, to do so on servers, because printer driver installation on a server may unintentionally cause the computer to become less stable. A malicious user could install inappropriate printer drivers in a deliberate attempt to damage the computer, or a user might accidentally install malicious software that masquerades as a printer driver. It is feasible for an attacker to disguise a Trojan horse program as a printer driver. The program may appear to users as if they must use it to print, but such a program could unleash malicious code on your computer network.

CCE Reference Number: CCE-37942-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.4.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Devices: Prevent users from installing printer drivers>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Disable all apps from Windows Store' is set to 'Enabled' — Trivial

Vulnerability Details

This setting configures the launch of all apps from the Windows Store that came pre-installed or were downloaded. The recommended state for this setting is: Enabled.

Rationale: The Store service is a retail outlet built into Windows, primarily for consumer use. In an enterprise environment the IT department should be managing the installation of all applications to reduce the risk of the installation of vulnerable software.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.61.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Disable all apps from Windows Store>

Impact: All apps from the Windows Store that came pre-installed or were downloaded are prevented from launching. Existing Windows Store apps will not be updated. Windows Store is disabled.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Disable pre-release features or settings' is set to 'Disabled' — Trivial

Vulnerability Details

This policy setting determines the level that Microsoft can experiment with the product to study user preferences or device behavior. A value of 1 permits Microsoft to configure device settings only. A value of 2 allows Microsoft to conduct full experimentations. The recommended state for this setting is: Disabled.

Rationale: It can be dangerous in an Enterprise environment if experimental features are allowed because this can introduce bugs and security holes into systems, making it easier for an attacker to gain access. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.16.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Disable pre-release features or settings Note: This Group Policy path does not exist by default. An additional Group Policy template (datacollection.admx/adml) is required - it is included with the Microsoft Windows 10 Administrative Templates. Impact: All experimentations will be turned off.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices Impact: If you enable this policy setting, AutoPlay is not allowed for MTP devices like cameras or phones.

Vulnerability Details

This policy setting disallows AutoPlay for MTP devices like cameras or phones. The recommended state for this setting is: Enabled.

Rationale: An attacker could use this feature to launch a program to damage a client computer or data on the computer.

CCE Reference Number: CCE-37636-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.8.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Disallow Autoplay for non-volume devices' is set to 'Enabled'	Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Disallow Autoplay for non-volume devices>

Impact: AutoPlay will not be allowed for MTP devices like cameras or phones.

Vulnerability Details

This policy setting disallows AutoPlay for MTP devices like cameras or phones. The recommended state for this setting is: Enabled.

Rationale: An attacker could use this feature to launch a program to damage a client computer or data on the computer.

CCE Reference Number: CCE-37636-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.8.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Disallow copying of user input methods to the system account for sign-in' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Locale Services\Disallow copying

of user input methods to the system account for sign-in>

Impact: Users will have input methods enabled for the system account on the sign-in page.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy prevents automatic copying of user input methods to the system account for use on the sign-in screen. The user is restricted to the set of input methods that are enabled in the system account. The recommended state for this setting is: Enabled.

Rationale: This is a way to increase the security of the system account.

CCE Reference Number: CCE-36343-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.24.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled'	Trivial

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication. If you enable this policy setting, the WinRM client will not use Digest authentication. If you disable or do not configure this policy setting, the WinRM client will use Digest authentication. The recommended state for this setting is: Enabled.

Rationale: Digest authentication is less robust than other authentication methods available in WinRM, an attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

CCE Reference Number: CCE-38318-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.81.1.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest authentication Impact: The WinRM client will not use Digest authentication.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Disallow Digest authentication' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\Disallow Digest authentication>

Impact: The WinRM client will not use Digest authentication.

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) client will not use Digest authentication. The recommended state for this setting is: Enabled.

Rationale: Digest authentication is less robust than other authentication methods available in WinRM, an attacker who is able to capture packets on the network where WinRM is running may be able to determine the credentials used for accessing remote hosts via WinRM.

CCE Reference Number: CCE-38318-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.86.1.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials Impact: The WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer. If this setting is later Disabled again, any values that were previously configured for RunAsPassword will need to be reset.

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not allow RunAs credentials to be stored for any plug-ins. If you enable this policy setting, the WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on this computer. If you disable or do not configure this policy setting, the WinRM service will allow the RunAsUser and RunAsPassword configuration values to be set for plug-ins and the RunAsPassword value will be stored securely. If you enable and then disable this policy setting, any values that were previously configured for RunAsPassword will need to be reset. The recommended state for this setting is: Enabled.

Rationale: Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

CCE Reference Number: CCE-36000-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.81.2.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Disallow WinRM from storing RunAs credentials' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service\Disallow WinRM from storing RunAs credentials>

Impact: The WinRM service will not allow the RunAsUser or RunAsPassword configuration values to be set for any plug-ins. If a plug-in has already set the RunAsUser and RunAsPassword configuration values, the RunAsPassword configuration value will be erased from the credential store on the computer. If this setting is later Disabled again, any values that were previously configured for RunAsPassword will need to be reset.

Vulnerability Details

This policy setting allows you to manage whether the Windows Remote Management (WinRM) service will not allow RunAs credentials to be stored for any plug-ins. The recommended state for this setting is: Enabled. Note: If you enable and then disable this policy setting, any values that were previously configured for RunAsPassword will need to be reset.

Rationale: Although the ability to store RunAs credentials is a convenient feature it increases the risk of account compromise slightly. For example, if you forget to lock your desktop before leaving it unattended for a few minutes another person could access not only the desktop of your computer but also any hosts you manage via WinRM with cached RunAs credentials.

CCE Reference Number: CCE-36000-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.86.2.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain controller: Allow server operators to schedule tasks' is set to 'Disabled' (DC only) — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Allow server operators to schedule tasks>

Impact: The impact should be small for most organizations. Users (including those in the Server Operators group) will still be able to create jobs by means of the Task Scheduler Wizard. However, those jobs will run in the context of the account that the user authenticates with when setting up the job.

Vulnerability Details

This policy setting determines whether members of the Server Operators group are allowed to submit jobs by means of the AT schedule facility. The impact of this policy setting configuration should be small for most organizations. Users, including those in the Server Operators group, will still be able to create jobs by means of the Task Scheduler Wizard, but those jobs will run in the context of the account with which the user authenticates when they set up the job.

Note: An AT Service Account can be modified to select a different account rather than the LOCAL SYSTEM account. To change the account, open System Tools, click Scheduled Tasks, and then click Accessories folder. Then click AT Service Account on the Advanced menu. The recommended state for this setting is: Disabled.

Rationale: If you enable this policy setting, jobs that are created by server operators by means of the AT service will execute in the context of the account that runs that service. By default, that is the local SYSTEM account. If you enable this policy setting, server operators could perform tasks that SYSTEM is able to do but that they would typically not be able to do, such as add their account to the local Administrators group.

CCE Reference Number: CCE-37848-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.5.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain controller: LDAP server signing requirements' is set to 'Require signing' (DC only)

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Require signing:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: LDAP server signing requirements>

Impact: Unless TLS\SSL is being used, the LDAP data signing option must be negotiated. Clients that do not support LDAP signing will be unable to run LDAP queries against the domain controllers. All

Windows 2000-based computers in your organization that are managed from Windows Server 2003-based or Windows XP-based computers and that use Windows NT Challenge/Response (NTLM) authentication must have Windows 2000 Service Pack 3 (SP3) installed. Alternatively, these clients must have a registry change. For information about this registry change, see Microsoft Knowledge Base article 325465: Windows 2000 domain controllers require SP3 or later when using Windows Server 2003 administration tools. Also, some non-Microsoft operating systems do not support LDAP signing. If you enable this policy setting, client computers that use those operating systems may be unable to access domain resources.

Vulnerability Details

This policy setting determines whether the Lightweight Directory Access Protocol (LDAP) server requires LDAP clients to negotiate data signing. Note: This policy setting does not have any impact on LDAP simple bind (ldap_simple_bind) or LDAP simple bind through SSL (ldap_simple_bind_s). No Microsoft LDAP clients that are shipped with Windows XP Professional use LDAP simple bind or LDAP simple bind through SSL to talk to a domain controller. The recommended state for this setting is: Require signing.

Rationale: Unsigned network traffic is susceptible to man-in-the-middle attacks. In such attacks, an intruder captures packets between the server and the client, modifies them, and then forwards them to the client. Where LDAP servers are concerned, an attacker could cause a client to make decisions that are based on false records from the LDAP directory. To lower the risk of such an intrusion in an organization's network, you can implement strong physical security measures to protect the network infrastructure. Also, you could implement Internet Protocol security (IPsec) authentication header mode (AH), which performs mutual authentication and packet integrity for IP traffic to make all types of man-in-the-middle attacks extremely difficult.

CCE Reference Number: CCE-35904-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.5.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain controller: Refuse machine account password changes' is set to 'Disabled' (DC only)

Trivial

Vulnerability Details

This security setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. The recommended state for this setting is: Disabled.

Rationale: If you enable this policy setting on all domain controllers in a domain, domain members will not be able to change their computer account passwords, and those passwords will be more susceptible to attack.

CCE Reference Number: CCE-36921-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.5.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain controller: Refuse machine account password changes>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always) Impact: Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:#x2022; The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.#x2022; Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.#x2022; The ability to authenticate other domains' users from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled.You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:#x2022; The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.#x2022; Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.#x2022; The ability to authenticate other domains' users from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled. You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.

Vulnerability Details

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted. If a system is set to always encrypt or sign secure channel data, it cannot establish a secure channel with a domain controller that is not capable of signing or encrypting all secure channel traffic, because all secure channel data must be signed and encrypted.Microsoft recommends to configure the Domain member: Digitally encrypt or sign secure channel data (always) setting to Enabled. The recommended state for this setting is: Enabled.

Rationale: When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated#x2014;and sensitive information such as passwords are encrypted#x2014;but the channel is not integrity-checked, and not all information is encrypted. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

CCE Reference Number: CCE-36142-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.6.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Digitally encrypt or sign secure channel data (always)' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt or sign secure channel data (always)>

Impact: None - this is the default configuration. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following: The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled. The ability to authenticate other domains' users from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled. You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a.

Vulnerability Details

This policy setting determines whether all secure channel traffic that is initiated by the domain member must be signed or encrypted. The recommended state for this setting is: Enabled.

Rationale: When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated and sensitive information such as passwords are encrypted but the channel is not integrity-checked, and not all information is encrypted. Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller.

CCE Reference Number: CCE-36142-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.6.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled' — Trivial

Vulnerability Details

This policy setting determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates. If you enable this policy setting, the domain member will request encryption of all secure channel traffic. If you disable this policy setting, the domain member will be prevented from negotiating secure channel encryption. Microsoft recommends to configure the Domain member: Digitally encrypt secure channel data (when possible) setting to Enabled. The recommended state for this setting is: Enabled.

Rationale: When a Windows Server 2003, Windows XP, Windows 2000, or Windows NT computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated#x2014;and sensitive information such as passwords are encrypted#x2014;but the channel is not integrity-checked, and not all information is encrypted. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

CCE Reference Number: CCE-37130-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.6.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible) Impact: Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Digitally encrypt secure channel data (when possible)' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally encrypt secure channel data (when possible)>

Impact: None - this is the default configuration. However, only Windows NT 4.0 Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed.

Vulnerability Details

This policy setting determines whether a domain member should attempt to negotiate encryption for all secure channel traffic that it initiates. The recommended state for this setting is: Enabled.

Rationale: When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated and sensitive information such as passwords are encrypted but the channel is not integrity-checked, and not all information is encrypted. Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller.

CCE Reference Number: CCE-37130-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.6.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally sign secure channel data (when possible) Impact: Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed. Therefore, you cannot enable the Domain member: Digitally encrypt or sign secure channel data (always) setting on domain controllers that support Windows 98 clients as members of the domain. Potential impacts can include the following:#x2022; The ability to create or delete trust relationships with clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.#x2022; Logons from clients running versions of Windows earlier than Windows NT 4.0 with SP6a will be disabled.#x2022; The ability to authenticate other domains' users from a domain controller running a version of Windows earlier than Windows NT 4.0 with SP6a in a trusted domain will be disabled.You can enable this policy setting after you eliminate all Windows 9x clients from the domain and upgrade all Windows NT 4.0 servers and domain controllers from trusted/trusting domains to Windows NT 4.0 with SP6a. You can enable the other two policy settings, Domain member: Digitally encrypt secure channel data (when possible) and Domain member: Digitally encrypt sign channel data (when possible), on all computers in the domain that support them and clients running versions of Windows earlier than Windows NT 4.0 with SP6a and applications that run on these versions of Windows will not be affected.

Vulnerability Details

This policy setting determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network.Microsoft recommends to configure the Domain member: Digitally sign secure channel data (when possible) setting to Enabled. The recommended state for this setting is: Enabled.

Rationale: When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated#x2014;and sensitive information such as passwords are encrypted#x2014;but the channel is not integrity-checked, and not all information is encrypted. If a computer is configured to always encrypt or sign secure channel data but the domain controller cannot sign or encrypt any portion of the secure channel data, the computer and domain controller cannot establish a secure channel. If the computer is configured to encrypt or sign secure channel data when possible, a secure channel can be established, but the level of encryption and signing is negotiated.

CCE Reference Number: CCE-37222-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.6.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Digitally sign secure channel data (when possible)' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting determines whether a domain member should attempt to negotiate whether all secure channel traffic that it initiates must be digitally signed. Digital signatures protect the traffic from being modified by anyone who captures the data as it traverses the network. The recommended state for this setting is: Enabled.

Rationale: When a computer joins a domain, a computer account is created. After it joins the domain, the computer uses the password for that account to create a secure channel with the domain controller for its domain every time that it restarts. Requests that are sent on the secure channel are authenticated and sensitive information such as passwords are encrypted but the channel is not integrity-checked, and not all information is encrypted. Digital encryption and signing of the secure channel is a good idea where it is supported. The secure channel protects domain credentials as they are sent to the domain controller.

CCE Reference Number: CCE-37222-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.6.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Digitally sign secure channel data (when possible)>

Impact: None - this is the default configuration. However, only Windows NT 4.0 with Service Pack 6a (SP6a) and subsequent versions of the Windows operating system support digital encryption and signing of the secure channel. Windows 98 Second Edition clients do not support it unless they have the Dsclient installed.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines whether a domain member can periodically change its computer account password. If you enable this policy setting, the domain member will be prevented from changing its computer account password. If you disable this policy setting, the domain member can change its computer account password as specified by the Domain Member: Maximum machine account password age setting, which by default is every 30 days. Computers that cannot automatically change their account passwords are potentially vulnerable, because an attacker might be able to determine the password for the system's domain account. The recommended state for this setting is: Disabled.

Rationale: The default configuration for Windows Server 2003 based computers that belong to a domain is that they are automatically required to change the passwords for their accounts every 30 days. If you disable this policy setting, computers that run Windows Server 2003 will retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk from an attacker who could determine the password for the computer's domain account.

CCE Reference Number: CCE-37508-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.6.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password changes Impact: None. This is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Disable machine account password changes' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines whether a domain member can periodically change its computer account password. Computers that cannot automatically change their account passwords are potentially vulnerable, because an attacker might be able to determine the password for the system's domain account. The recommended state for this setting is: Disabled.

Rationale: The default configuration for Windows Server 2003-based computers that belong to a domain is that they are automatically required to change the passwords for their accounts every 30 days. If you disable this policy setting, computers that run Windows Server 2003 will retain the same passwords as their computer accounts. Computers that are no longer able to automatically change their account password are at risk from an attacker who could determine the password for the computer's domain account.

CCE Reference Number: CCE-37508-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.6.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Disable machine account password changes>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 30 or fewer days, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age Impact: None. This is the default configuration.

Vulnerability Details

This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days. If you increase this interval significantly so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts. The recommended state for this setting is: 30 or fewer days, but not 0.

Note: A value of 0 does not conform to the benchmark as it disables maximum password age.

Rationale: In Active Directory-based domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker will have more time to undertake a brute force attack to guess the password of one or more computer accounts.

CCE Reference Number: CCE-37431-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.6.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Maximum machine account password age' is set to '30 or fewer days, but not 0' — Trivial

Vulnerability Details

This policy setting determines the maximum allowable age for a computer account password. By default, domain members automatically change their domain passwords every 30 days. If you increase this interval significantly so that the computers no longer change their passwords, an attacker would have more time to undertake a brute force attack against one of the computer accounts. The recommended state for this setting is: 30 or fewer days, but not 0.

Note: A value of 0 does not conform to the benchmark as it disables maximum password age.

Rationale: In Active Directory-based domains, each computer has an account and password just like every user. By default, the domain members automatically change their domain password every 30 days. If you increase this interval significantly, or set it to 0 so that the computers no longer change their passwords, an attacker will have more time to undertake a brute force attack to guess the password of one or more computer accounts.

CCE Reference Number: CCE-37431-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.6.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to 30 or fewer days, but not 0:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Maximum machine account password age>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key Impact: Computers that have this policy setting enabled will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly. Also, computers that do not support this policy setting will not be able to join domains in which the domain controllers have this policy setting enabled.

Vulnerability Details

When this policy setting is enabled, a secure channel can only be established with domain controllers that are capable of encrypting secure channel data with a strong (128-bit) session key. To enable this policy setting, all domain controllers in the domain must be able to encrypt secure channel data with a strong key, which means all domain controllers must be running Microsoft Windows 2000 or later. If communication to non-Windows 2000 based domains is required, it is recommended that you disable this policy setting. The recommended state for this setting is: Enabled.

Rationale: Session keys that are used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping. (Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or be redirected.)

CCE Reference Number: CCE-37614-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.6.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Domain member: Require strong (Windows 2000 or later) session key' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Domain member: Require strong (Windows 2000 or later) session key>

Impact: None - this is the default configuration. However, computers will not be able to join Windows NT 4.0 domains, and trusts between Active Directory domains and Windows NT-style domains may not work properly. Also, domain controllers with this setting configured will not allow older pre-Windows 2000 clients (that that do not support this policy setting) to join the domain.

Vulnerability Details

When this policy setting is enabled, a secure channel can only be established with domain controllers that are capable of encrypting secure channel data with a strong (128-bit) session key. To enable this policy setting, all domain controllers in the domain must be able to encrypt secure channel data with a strong key, which means all domain controllers must be running Microsoft Windows 2000 or later. The recommended state for this setting is: Enabled.

Rationale: Session keys that are used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems. Whenever possible, you should take advantage of these stronger session keys to help protect secure channel communications from attacks that attempt to hijack network sessions and eavesdropping. (Eavesdropping is a form of hacking in which network data is read or altered in transit. The data can be modified to hide or change the sender, or be redirected.)

CCE Reference Number: CCE-37614-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.6.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not allow COM port redirection' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting specifies whether to prevent the redirection of data to client COM ports from the remote computer in a Remote Desktop Services session. The recommended state for this setting is: Enabled.

Rationale: In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for COM port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

CCE Reference Number: CCE-37696-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.3.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow COM port redirection>

Impact: Users in a Remote Desktop Services session will not be able to redirect server data to local (client) COM ports.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection Impact: Drive redirection will not be possible. In most cases, traditional network drive mapping to file shares (including administrative shares) will serve as a capable substitute to still allow file transfers when needed.

Vulnerability Details

This policy setting prevents users from sharing the local drives on their client computers to Terminal Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format: \\TSClient\ <driveletter> $

If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them. The recommended state for this setting is: Enabled.

Rationale: Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction.

CCE Reference Number: CCE-36509-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.48.3.3.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not allow drive redirection' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow drive redirection>

Impact: Drive redirection will not be possible. In most situations, traditional network drive mapping to file shares (including administrative shares) performed manually by the connected user will serve as a capable substitute to still allow file transfers when needed.

Vulnerability Details

This policy setting prevents users from sharing the local drives on their client computers to Terminal Servers that they access. Mapped drives appear in the session folder tree in Windows Explorer in the following format: \\TSClient\<driveletter>$ If local drives are shared they are left vulnerable to intruders who want to exploit the data that is stored on them. The recommended state for this setting is: Enabled.

Rationale: Data could be forwarded from the user's Terminal Server session to the user's local computer without any direct user interaction. Malicious software already present on a compromised server would have direct and stealthy disk access to the user's local computer during the Remote Desktop session.

CCE Reference Number: CCE-36509-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.3.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not allow LPT port redirection' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow LPT port redirection>

Impact: Users in a Remote Desktop Services session will not be able to redirect server data to local (client) LPT ports.

Vulnerability Details

This policy setting specifies whether to prevent the redirection of data to client LPT ports during a Remote Desktop Services session. The recommended state for this setting is: Enabled.

Rationale: In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for LPT port redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

CCE Reference Number: CCE-37778-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.3.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only)	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: When you enable this setting, planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not allow password expiration time longer than required by policy' is set to 'Enabled' (MS only)	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\LAPS\Do not allow password expiration time longer than required by policy

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: Planned password expiration longer than password age dictated by "Password Settings" policy is NOT allowed.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.2.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client\Do not allow passwords to be saved Impact: If you enable this policy setting, the password saving checkbox is disabled for Remote Desktop Services / Terminal Services clients and users will not be able to save passwords.

Vulnerability Details

This policy setting helps prevent Remote Desktop Services / Terminal Services clients from saving passwords on a computer. Note If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Terminal Services client disconnects from any server. The recommended state for this setting is: Enabled.

Rationale: An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker who compromises a user's account and connects to their computer could use saved passwords to gain access to additional hosts.

CCE Reference Number: CCE-36223-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.48.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not allow passwords to be saved' is set to 'Enabled'	Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client\Do not allow passwords to be saved>

Impact: The password saving checkbox will be disabled for Remote Desktop Services / Terminal Services clients and users will not be able to save passwords.

Vulnerability Details

This policy setting helps prevent Remote Desktop Services / Terminal Services clients from saving passwords on a computer. The recommended state for this setting is: Enabled.

Note: If this policy setting was previously configured as Disabled or Not configured, any previously saved passwords will be deleted the first time a Terminal Services client disconnects from any server.

Rationale: An attacker with physical access to the computer may be able to break the protection guarding saved passwords. An attacker who compromises a user's account and connects to their computer could use saved passwords to gain access to additional hosts.

CCE Reference Number: CCE-36223-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.2.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not allow supported Plug and Play device redirection' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\Do not allow supported Plug and Play device redirection>

Impact: Users in a Remote Desktop Services session will not be able to redirect their supported (local client) Plug and Play devices to the remote computer.

Vulnerability Details

This policy setting allows you to control the redirection of supported Plug and Play devices, such as Windows Portable Devices, to the remote computer in a Remote Desktop Services session. The recommended state for this setting is: Enabled.

Rationale: In a more security-sensitive environment, it is desirable to reduce the possible attack surface. The need for Plug and Play device redirection within a Remote Desktop session is very rare, so makes sense to reduce the number of unexpected avenues for data exfiltration and/or malicious code transfer.

CCE Reference Number: CCE-37477-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.3.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

Trivial

Vulnerability Details

This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff. The recommended state for this setting is: Disabled .

Rationale: Sensitive information could be contained inside the temporary folders and shared with other administrators that log into the system.

CCE Reference Number: CCE-37946-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.48.3.11.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer

Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Do not delete temp folders upon exit Impact: If you disable this policy setting, temporary folders are deleted when a user logs off, even if the server administrator specifies otherwise.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not delete temp folders upon exit' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not delete temp folders upon exit>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting specifies whether Remote Desktop Services retains a user's per-session temporary folders at logoff. The recommended state for this setting is: Disabled.

Rationale: Sensitive information could be contained inside the temporary folders and shared with other administrators that log into the system.

CCE Reference Number: CCE-37946-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.11.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled'

Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Enabled: Computer Configuration\Policies\Administrative Templates\System\Logon\Do not display network selection UI Impact: If you enable this policy setting, the PC's network connectivity state cannot be changed without signing into Windows. If you disable or don't configure this policy setting, any user can disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting allows you to control whether anyone can interact with available networks UI on the logon screen. The recommended state for this setting is: Enabled.

Rationale: An unauthorized user could disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

CCE Reference Number: CCE-38353-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.24.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not display network selection UI' is set to 'Enabled'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Logon\Do not display network selection UI>

Impact: The PC's network connectivity state cannot be changed without signing into Windows.

Vulnerability Details

This policy setting allows you to control whether anyone can interact with available networks UI on the logon screen. The recommended state for this setting is: Enabled.

Rationale: An unauthorized user could disconnect the PC from the network or can connect the PC to other available networks without signing into Windows.

CCE Reference Number: CCE-38353-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.25.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting allows you to configure the display of the password reveal button in password entry user experiences. The recommended state for this setting is: Enabled.

Rationale: This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

CCE Reference Number: CCE-37534-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.13.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Do not display the password reveal button Impact: If you enable this policy setting the password reveal button will not be displayed after a user types a password in the password entry text box. If you disable or do not configure this policy setting the password reveal button will be displayed after a user types a password in the password entry text box. The policy applies to all Windows components and applications that use the Windows system controls including Internet Explorer.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not display the password reveal button' is set to 'Enabled'	Trivial

Vulnerability Details

This policy setting allows you to configure the display of the password reveal button in password entry user experiences. The recommended state for this setting is: Enabled.

Rationale: This is a useful feature when entering a long and complex password, especially when using a touchscreen. The potential risk is that someone else may see your password while surreptitiously observing your screen.

CCE Reference Number: CCE-37534-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.15.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Do not display the password reveal button>

Impact: The password reveal button will not be displayed after a user types a password in the password entry text box.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Logon\Do not enumerate connected users on domain-joined computers Impact: The Logon UI will not enumerate any connected users on domain-joined computers.

Vulnerability Details

This policy setting prevents connected users from being enumerated on domain-joined computers. If you enable this policy setting, the Logon UI will not enumerate any connected users on domain-joined computers. If you disable or do not configure this policy setting, connected users will be enumerated on domain-joined computers. The recommended state for this setting is: Enabled.

Rationale: A malicious user could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

CCE Reference Number: CCE-37838-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.24.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not enumerate connected users on domain-joined computers' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting prevents connected users from being enumerated on domain-joined computers. The recommended state for this setting is: Enabled.

Rationale: A malicious user could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

CCE Reference Number: CCE-37838-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.25.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Logon\Do not enumerate connected users on domain-joined computers>

Impact: The Logon UI will not enumerate any connected users on domain-joined computers.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not preserve zone information in file attachments' is set to 'Disabled'

Trivial

Vulnerability Details

This policy setting allows you to manage whether Windows marks file attachments from Internet Explorer or Microsoft Outlook' Express with information about their zone of origin (such as restricted, Internet, intranet, or local). This policy setting requires that files be downloaded to NTFS disk partitions to function correctly. If zone information is not preserved, Windows cannot make proper risk assessments based on the zone where the attachment came from. If the Do not preserve zone information in file attachments setting is enabled, file attachments are not marked with their zone information. If this policy setting is disabled, Windows is forced to store file attachments with their zone information. The recommended state for this setting is: Disabled.

Rationale: A file that is downloaded from a computer in the Internet or Restricted Sites zone may be moved to a location that makes it appear safe, like an intranet file share, and executed by an unsuspecting user.

CCE Reference Number: CCE-37424-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 19.7.4.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Do not preserve zone information in file attachments Impact: None, this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not show feedback notifications' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Do not show feedback notifications>

Impact: Users will no longer see feedback notifications through the Windows Feedback app.

Vulnerability Details

This policy setting allows an organization to prevent its devices from showing feedback questions from Microsoft. The recommended state for this setting is: Enabled.

Rationale: In an enterprise environment users should not be sending any feedback to 3rd party vendors. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.16.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Temporary Folders\Do not use temporary folders per session Impact: If this setting is enabled, only one temporary folder is used for all remote sessions. If a communal temporary folder is used, it might be possible for users to access other users temporary folders.

Vulnerability Details

By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the "sessionid." This temporary folder is used to store individual temporary files. To reclaim disk space, the temporary folder is deleted when the user logs off from a session. The recommended state for this setting is: Disabled.

Rationale: By Disabling this setting you are keeping the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

CCE Reference Number: CCE-38180-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.48.3.11.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Do not use temporary folders per session' is set to 'Disabled'

Trivial

Vulnerability Details

By default, Remote Desktop Services creates a separate temporary folder on the RD Session Host server for each active session that a user maintains on the RD Session Host server. The temporary folder is created on the RD Session Host server in a Temp folder under the user's profile folder and is named with the "sessionid." This temporary folder is used to store individual temporary files. To reclaim disk space, the temporary folder is deleted when the user logs off from a session. The recommended state for this setting is: Disabled.

Rationale: By Disabling this setting you are keeping the cached data independent for each session, both reducing the chance of problems from shared cached data between sessions, and keeping possibly sensitive data separate to each user session.

CCE Reference Number: CCE-38180-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.11.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop

Services\Remote Desktop Session Host\Temporary Folders\Do not use temporary folders per session>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'EMET 5.5' or higher is installed — Trivial

Vulnerability Details

The Enhanced Mitigation Experience Toolkit (EMET) is free, supported, software developed by Microsoft that allows an enterprise to apply exploit mitigations to applications that run on Windows.

Rationale: EMET mitigations help reduce the reliability of exploits that target vulnerable software running on Windows CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.22.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Install EMET 5.5 or higher.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable/Disable PerfTrack' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and

Diagnostics\Windows Performance PerfTrack\Enable/Disable PerfTrack>

Impact: Responsiveness events are not processed.

Vulnerability Details

This policy setting specifies whether to enable or disable tracking of responsiveness events. The recommended state for this setting is: Disabled.

Rationale: When enabled the aggregated data of a given event will be transmitted to Microsoft. The option exists to restrict this feature for a specific user, set the consent level, and designate specific programs for which error reports could be sent. However, centrally restricting the ability to execute PerfTrack to limit the potential for unauthorized or undesired usage, data leakage, or unintentional communications is highly recommended.

CCE Reference Number: CCE-36648-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.39.11.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable Font Providers' is set to 'Disabled' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Network\Fonts\Enable Font Providers

Note: This Group Policy path does not exist by default. An updated Group Policy template (GroupPolicy.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Impact: Windows will not connect to an online font provider and will only enumerate locally-installed fonts.

Vulnerability Details

This policy setting determines whether Windows is allowed to download fonts and font catalog data from an online font provider. The recommended state for this setting is: Disabled.

Rationale: In an enterprise environment the IT department should be managing the changes to the system configuration, to ensure all changes are tested and approved.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.5.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable insecure guest logons' is set to 'Disabled' | Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Network\Lanman Workstation\Enable insecure guest logons

Note: This Group Policy path does not exist by default. It is included with the Group Policy template (lanmanworkstation.admx/adml) that is included with the Microsoft Windows 10 Administrative Templates (or newer). Impact: The SMB client will reject insecure guest logons.

Vulnerability Details

This policy setting determines if the SMB client will allow insecure guest logons to an SMB server. The recommended state for this setting is: Disabled.

Rationale: Insecure guest logons are used by file servers to allow unauthenticated access to shared folders. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.8.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only) | Trivial

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.2.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: If you enable this setting, local administrator password is managed. If you disable or not configure this setting, local administrator password is NOT managed. In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable Local Admin Password Management' is set to 'Enabled' (MS only)

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\LAPS\Enable Local Admin Password Management

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: The local administrator password is managed (provided that the LAPS AdmPwd GPO Extension / CSE is installed on the target computer (see rule 18.2.1), the Active Directory domain schema and account permissions have been properly configured on the domain). In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.2.3

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)	Trivial

Vulnerability Details

This policy setting controls whether RPC clients authenticate with the Endpoint Mapper Service when the call they are making contains authentication information. The Endpoint Mapper Service on computers running Windows NT4 (all service packs) cannot process authentication information supplied in this manner. This policy setting can cause a specific issue with 1-way forest trusts if it is applied to the trusting domain DCs (see Microsoft KB3073942), so we do not recommend applying it to domain controllers. If you disable this policy setting, RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Endpoint Mapper Service on Windows NT4 Server. If you enable this policy setting, RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service. If you do not configure this policy setting, it remains disabled. RPC clients will not authenticate to the Endpoint Mapper Service, but they will be able to communicate with the Windows NT4 Server Endpoint Mapper Service.

Note: This policy will not be applied until the system is rebooted. The recommended state for this setting is: Enabled.

Rationale: Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.

CCE Reference Number: CCE-37346-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.31.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication Impact: RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable RPC Endpoint Mapper Client Authentication' is set to 'Enabled' (MS only)

Trivial

Vulnerability Details

This policy setting controls whether RPC clients authenticate with the Endpoint Mapper Service when the call they are making contains authentication information. The Endpoint Mapper Service on computers running Windows NT4 (all service packs) cannot process authentication information supplied in this manner. This policy setting can cause a specific issue with 1-way forest trusts if it is applied to the trusting domain DCs (see Microsoft KB3073942), so we do not recommend applying it to domain controllers.

Note: This policy will not be applied until the system is rebooted. The recommended state for this setting is: Enabled.

Rationale: Anonymous access to RPC services could result in accidental disclosure of information to unauthenticated users.

CCE Reference Number: CCE-37346-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.32.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Enable RPC Endpoint Mapper Client Authentication>

Impact: RPC clients will authenticate to the Endpoint Mapper Service for calls that contain authentication information. Clients making such calls will not be able to communicate with the Windows NT4 Server Endpoint Mapper Service.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable screen saver' is set to 'Enabled' — Trivial

Vulnerability Details

This policy setting allows you to manage whether or not screen savers run. If the Screen Saver setting is disabled screen savers do not run and the screen saver section of the Screen Saver tab in Display in Control Panel is disabled. If this setting is enabled a screen saver will run if the following two conditions are met: first, that a valid screen saver is specified on the client via the Screen Saver Executable Name group policy setting or Control Panel on the client. Second, the screensaver timeout is set to a value greater than zero via the Screen Saver Timeout group policy setting or Control Panel on the client. The recommended state for this setting is: Enabled.

Rationale: If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

CCE Reference Number: CCE-37970-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 19.1.3.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Enable screen saver
Impact: The screen saver will automatically activate when the computer has been unattended for the amount of time specified by the Screen Saver timeout setting. The impact should be minimal since the screen saver is enabled by default.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable Windows NTP Client' is set to 'Enabled' — Trivial

Vulnerability Details

This policy setting specifies whether the Windows NTP Client is enabled. Enabling the Windows NTP Client allows your computer to synchronize its computer clock with other NTP servers. You might want to disable this service if you decide to use a third-party time provider. The recommended state for this setting is: Enabled.

Rationale: A reliable and accurate account of time is important for a number of services and security requirements, including but not limited to distributed applications, authentication services, multi-user databases and logging services. The use of an NTP client (with secure operation) establishes functional accuracy and is a focal point when reviewing security relevant events

CCE Reference Number: CCE-37843-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.44.1.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Client>

Impact: You can set the local computer clock to synchronize time with NTP servers.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enable Windows NTP Server' is set to 'Disabled' (MS only) — Trivial

Vulnerability Details

This policy setting allows you to specify whether the Windows NTP Server is enabled. The recommended state for this setting is: Disabled.

Rationale: The configuration of proper time synchronization is critically important in a corporate environment both due to the sensitivity of Kerberos authentication timestamps and also to ensure accurate security logging.

CCE Reference Number: CCE-37319-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.44.1.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\Enable Windows NTP Server>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history Impact: The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: 24 or more password(s).

Rationale: The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

CCE Reference Number: CCE-37166-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 1.1.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enforce password history' is set to '24 or more password(s)'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 24 or more password(s):

<Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Enforce password history>

Impact: The major impact of this configuration is that users must create a new password every time they are required to change their old one. If users are required to change their passwords to new unique values, there is an increased risk of users who write their passwords somewhere so that they do not forget them. Another risk is that users may create passwords that change incrementally (for example, password01, password02, and so on) to facilitate memorization but make them easier to guess. Also, an excessively low value for the Minimum password age setting will likely increase administrative overhead, because users who forget their passwords might ask the help desk to reset them frequently.

Vulnerability Details

This policy setting determines the number of renewed, unique passwords that have to be associated with a user account before you can reuse an old password. The value for this policy setting must be between 0 and 24 passwords. The default value for Windows Vista is 0 passwords, but the default setting in a domain is 24 passwords. To maintain the effectiveness of this policy setting, use the Minimum password age setting to prevent users from repeatedly changing their password. The recommended state for this setting is: 24 or more password(s).

Rationale: The longer a user uses the same password, the greater the chance that an attacker can determine the password through brute force attacks. Also, any accounts that may have been compromised will remain exploitable for as long as the password is left unchanged. If password changes are required but password reuse is not prevented, or if users continually reuse a small number of passwords, the effectiveness of a good password policy is greatly reduced. If you specify a low number for this policy setting, users will be able to use the same small number of passwords repeatedly. If you do not also configure the Minimum password age setting, users might repeatedly change their passwords until they can reuse their original password.

CCE Reference Number: CCE-37166-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 1.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation Impact: If you enable this policy setting, all local administrator accounts on the machine will be displayed so the user can choose one and enter the correct password. If you disable this policy setting, users will be required to always type in a username and password to elevate.

Vulnerability Details

By default, all administrator accounts are displayed when you attempt to elevate a running application. The recommended state for this setting is: Disabled.

Rationale: Users could see the list of administrator accounts, making it slightly easier for a malicious user who has logged onto a console session to try to crack the passwords of those accounts.

CCE Reference Number: CCE-36512-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.13.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enumerate administrator accounts on elevation' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\Enumerate administrator accounts on elevation>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting controls whether administrator accounts are displayed when a user attempts to elevate a running application. The recommended state for this setting is: Disabled.

Rationale: Users could see the list of administrator accounts, making it slightly easier for a malicious user who has logged onto a console session to try to crack the passwords of those accounts.

CCE Reference Number: CCE-36512-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.15.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled'

Trivial

Vulnerability Details

This policy setting allows local users to be enumerated on domain-joined computers. If you enable this policy setting, Logon UI will enumerate all local users on domain-joined computers. If you disable or do not configure this policy setting, the Logon UI will not enumerate local users on domain-joined computers. The recommended state for this setting is: Disabled.

Rationale: A malicious user could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

CCE Reference Number: CCE-35894-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.24.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Logon\Enumerate local users on domain-joined computers Impact: None - this is the default behavior.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Enumerate local users on domain-joined computers' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting allows local users to be enumerated on domain-joined computers. The recommended state for this setting is: Disabled.

Rationale: A malicious user could use this feature to gather account names of other users, that information could then be used in conjunction with other types of attacks such as guessing passwords or social engineering. The value of this countermeasure is small because a user with domain credentials could gather the same account information using other methods.

CCE Reference Number: CCE-35894-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.25.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\System\Logon\Enumerate local users on domain-joined computers>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators'	Trivial

Vulnerability Details

This policy setting allows users to shut down Windows Vista-based computers from remote locations on the network. Anyone who has been assigned this user right can cause a denial of service (DoS) condition, which would make the computer unavailable to service user requests. Therefore, it is recommended that only highly trusted administrators be assigned this user right. The recommended state for this setting is: Administrators.

Rationale: Any user who can shut down a computer could cause a DoS condition to occur. Therefore, this user right should be tightly restricted.

CCE Reference Number: CCE-37877-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.23

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system Impact: If you remove the Force shutdown from a remote system user right from the Server Operator group you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Force shutdown from a remote system' is set to 'Administrators'

Trivial

Vulnerability Details

This policy setting allows users to shut down Windows Vista-based computers from remote locations on the network. Anyone who has been assigned this user right can cause a denial of service (DoS) condition, which would make the computer unavailable to service user requests. Therefore, it is recommended that only highly trusted administrators be assigned this user right. The recommended state for this setting is: Administrators.

Rationale: Any user who can shut down a computer could cause a DoS condition to occur. Therefore, this user right should be tightly restricted.

CCE Reference Number: CCE-37877-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.23

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Force shutdown from a remote system>

Impact: If you remove the Force shutdown from a remote system user right from the Server Operator group you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should confirm that delegated activities will not be adversely affected.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Force specific screen saver: Screen saver executable name' is set to 'Enabled: scrnsave.scr'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: scrnsave.scr: User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Force specific screen saver Impact: The screen saver will automatically activate when the computer has been unattended for the amount of time specified by the Screen Saver timeout setting.

Vulnerability Details

This policy setting allows you to manage whether or not screen savers run. If the Screen Saver setting is disabled screen savers do not run and the screen saver section of the Screen Saver tab in Display in Control Panel is disabled. If this setting is enabled a screen saver will run if the following two conditions are met: first, that a valid screen saver is specified on the client via the Screen Saver Executable Name group policy setting or Control Panel on the client. Second, the screensaver timeout is set to a value greater than zero via the Screen Saver Timeout group policy setting or Control Panel on the client. The recommended state for this setting is: Enabled: scrnsave.scr.

Rationale: If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

CCE Reference Number: CCE-37907-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 19.1.3.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits Impact: On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

Vulnerability Details

This policy setting determines which users or processes can generate audit records in the Security log. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE.

Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #2: A server that holds the Active Directory Federation Services Role will require a special exception to this recommendation, to allow the NT SERVICE\ADFSSrv and NT SERVICE\DRS services, as well as the associated Active Directory Federation Services service account, to be granted this user right.

Rationale: An attacker could use this capability to create a large number of audited events, which would make it more difficult for a system administrator to locate any illicit activity. Also, if the event log is configured to overwrite events as needed, any evidence of unauthorized activities could be overwritten by a large number of unrelated events.

CCE Reference Number: CCE-37639-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.24

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Generate security audits' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Generate security audits>

Impact: On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

Vulnerability Details

This policy setting determines which users or processes can generate audit records in the Security log. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE.

Note: A Member Server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #2: A Member Server that holds the Active Directory Federation Services Role will require a special exception to this recommendation, to allow the NT SERVICE\ADFSSrv and NT SERVICE\DRS services, as well as the associated Active Directory Federation Services service account, to be granted this user right.

Rationale: An attacker could use this capability to create a large number of audited events, which would make it more difficult for a system administrator to locate any illicit activity. Also, if the event log is configured to overwrite events as needed, any evidence of unauthorized activities could be overwritten by a large number of unrelated events.

CCE Reference Number: CCE-37639-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.24

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled with the following paths configured, at a minimum: \\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 \\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths Note: This Group Policy path does not exist by default. An additional Group Policy template (NetworkProvider.admx/adml) is required - it is included with KB3000483 or with the Microsoft Windows 10 Administrative Templates. Impact: If you enable this policy, Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

Vulnerability Details

This policy setting configures secure access to UNC paths. The recommended state for this setting is: Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares. Note: If the environment exclusively contains Windows 8.0 / Server 2012 or higher systems, then the "Privacy" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing.

Rationale: In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of MS15-011 / MSKB 3000483. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Vista/Server 2008 or higher (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (NetworkProvider.admx/adml) was also provided with the security update. Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk: \\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Note: A reboot may be required after the setting is applied to a client machine to access the above paths. Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014. CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.4.13.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Hardened UNC Paths' is set to 'Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares'

Trivial

Vulnerability Details

This policy setting configures secure access to UNC paths. The recommended state for this setting is: Enabled, with "Require Mutual Authentication" and "Require Integrity" set for all NETLOGON and SYSVOL shares.

Note: If the environment exclusively contains Windows 8.0 / Server 2012 or higher systems, then the "Privacy" setting may (optionally) also be set to enable SMB encryption. However, using SMB encryption will render the targeted share paths completely inaccessible by older OSes, so only use this additional option with caution and thorough testing.

Rationale: In February 2015, Microsoft released a new control mechanism to mitigate a security risk in Group Policy as part of MS15-011 / MSKB 3000483. This mechanism requires both the installation of the new security update and also the deployment of specific group policy settings to all computers on the domain from Vista/Server 2008 or higher (the associated security patch to enable this feature was not released for Server 2003). A new group policy template (NetworkProvider.admx/adml) was also provided with the security update. Once the new GPO template is in place, the following are the minimum requirements to remediate the Group Policy security risk: \\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 \\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1

Note: A reboot may be required after the setting is applied to a client machine to access the above paths. Additional guidance on the deployment of this security setting is available from the Microsoft Premier Field Engineering (PFE) Platforms TechNet Blog here: Guidance on Deployment of MS15-011 and MS15-014. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.14.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled with the following paths configured, at a minimum: \\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1 \\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1 Computer Configuration\Policies\Administrative Templates\Network\Network Provider\Hardened UNC Paths

Note: This Group Policy path does not exist by default. An additional Group Policy template (NetworkProvider.admx/adml) is required - it is included with KB3000483 or with the Microsoft Windows 10 Administrative Templates. Impact: Windows only allows access to the specified UNC paths after fulfilling additional security requirements.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines what information is logged in security audit events when a new process has been created. The recommended state for this setting is: Disabled.

Rationale: When this policy setting is enabled, any user who has read access to the security events can read the command-line arguments for any successfully created process. Command-line arguments may contain sensitive or private information such as passwords or user data.

CCE Reference Number: CCE-36925-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.2.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events Impact: If you disable or do not configure this policy setting, the process's command line information will not be included in Audit Process Creation events.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Include command line in process creation events' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines what information is logged in security audit events when a new process has been created. The recommended state for this setting is: Disabled.

Rationale: When this policy setting is enabled, any user who has read access to the security events can read the command-line arguments for any successfully created process. Command-line arguments may contain sensitive or private information such as passwords or user data.

CCE Reference Number: CCE-36925-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.3.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\System\Audit Process Creation\Include command line in process creation events>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators'

Trivial

Vulnerability Details

This policy setting determines whether users can increase the base priority class of a process. (It is not a privileged operation to increase relative priority within a priority class.) This user right is not required by administrative tools that are supplied with the operating system but might be required by software development tools. The recommended state for this setting is: Administrators.

Rationale: A user who is assigned this user right could increase the scheduling priority of a process to Real-Time, which would leave little processing time for all other processes and could lead to a DoS condition.

CCE Reference Number: CCE-38326-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.26

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority Impact: None. This is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Increase scheduling priority' is set to 'Administrators'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Increase scheduling priority>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting determines whether users can increase the base priority class of a process. (It is not a privileged operation to increase relative priority within a priority class.) This user right is not required by administrative tools that are supplied with the operating system but might be required by software development tools. The recommended state for this setting is: Administrators.

Rationale: A user who is assigned this user right could increase the scheduling priority of a process to Real-Time, which would leave little processing time for all other processes and could lead to a DoS condition.

CCE Reference Number: CCE-38326-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.26

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name Impact: Users will not see their user name or domain name when unlocking their computer, they will have to enter that information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: Enabled.

Rationale: An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

CCE Reference Number: CCE-36056-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.7.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Do not display last user name' is set to 'Enabled' — Trivial

Vulnerability Details

This policy setting determines whether the account name of the last user to log on to the client computers in your organization will be displayed in each computer's respective Windows logon screen. Enable this policy setting to prevent intruders from collecting account names visually from the screens of desktop or laptop computers in your organization. The recommended state for this setting is: Enabled.

Rationale: An attacker with access to the console (for example, someone with physical access or someone who is able to connect to the server through Terminal Services) could view the name of the last user who logged on to the server. The attacker could then try to guess the password, use a dictionary, or use a brute-force attack to try and log on.

CCE Reference Number: CCE-36056-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.7.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not display last user name>

Impact: The name of the last user to successfully log on is not be displayed in the Windows logon screen.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'

Trivial

Vulnerability Details

This policy setting determines whether users must press CTRL+ALT+DEL before they log on. If you enable this policy setting, users can log on without this key combination. If you disable this policy setting, users must press CTRL+ALT+DEL before they log on to Windows unless they use a smart card for Windows logon. A smart card is a tamper-proof device that stores security information. The recommended state for this setting is: Disabled.

Rationale: Microsoft developed this feature to make it easier for users with certain types of physical impairments to log on to computers that run Windows. If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path. An attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The attacker would then be able to log on to the compromised account with whatever level of privilege that user has.

CCE Reference Number: CCE-37637-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.7.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL Impact: Unless they use a smart card to log on, users will have to simultaneously press three keys before the logon dialog box will display.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Do not require CTRL+ALT+DEL' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL>

Impact: Users must press CTRL+ALT+DEL before they log on to Windows unless they use a smart card for Windows logon. A smart card is a tamper-proof device that stores security information.

Vulnerability Details

This policy setting determines whether users must press CTRL+ALT+DEL before they log on. The recommended state for this setting is: Disabled.

Rationale: Microsoft developed this feature to make it easier for users with certain types of physical impairments to log on to computers that run Windows. If users are not required to press CTRL+ALT+DEL, they are susceptible to attacks that attempt to intercept their passwords. If CTRL+ALT+DEL is required before logon, user passwords are communicated by means of a trusted path. An attacker could install a Trojan horse program that looks like the standard Windows logon dialog box and capture the user's password. The attacker would then be able to log on to the compromised account with whatever level of privilege that user has.

CCE Reference Number: CCE-37637-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.7.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' | Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 900 or fewer seconds, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit Impact: The screen saver will automatically activate when the computer has been unattended for the amount of time specified. The impact should be minimal since the screen saver is enabled by default.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session. The recommended state for this setting is: 900 or fewer second(s), but not 0.

Note: A value of 0 does not conform to the benchmark as it disables the machine inactivity limit.

Rationale: If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

CCE Reference Number: CCE-38235-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.7.3

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Machine inactivity limit' is set to '900 or fewer second(s), but not 0' | Trivial

Vulnerability Details

Windows notices inactivity of a logon session, and if the amount of inactive time exceeds the inactivity limit, then the screen saver will run, locking the session. The recommended state for this setting is: 900 or fewer second(s), but not 0.

Note: A value of 0 does not conform to the benchmark as it disables the machine inactivity limit.

Rationale: If a user forgets to lock their computer when they walk away it's possible that a passerby will hijack it.

CCE Reference Number: CCE-38235-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.7.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to 900 or fewer seconds, but not 0:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Machine inactivity limit>

Impact: The screen saver will automatically activate when the computer has been unattended for the amount of time specified. The impact should be minimal since the screen saver is enabled by default.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Number of previous logons to cache (in case domain controller is not available)' is set to '4 or fewer logon(s)' (MS only)

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 4 or fewer logon(s):

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Number of previous logons to cache (in case domain controller is not available)>

Impact: Users will be unable to log on to any computers if there is no domain controller available to authenticate them. Organizations may want to configure this value to 2 for end-user computers, especially for mobile users. A configuration value of 2 means that the user's logon information will still be in the cache, even if a member of the IT department has recently logged on to their computer to perform system maintenance. This method allows users to log on to their computers when they are not connected to the organization's network.

Vulnerability Details

This policy setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally to allow users to log on even if a domain controller cannot be contacted. This policy setting determines the number of unique users for whom logon information is cached locally. If this value is set to 0, the logon cache feature is disabled. An attacker who is able to access the file system of the server could locate this cached information and use a brute force attack to determine user passwords. The recommended state for this setting is: 4 or fewer logon(s).

Rationale: The number that is assigned to this policy setting indicates the number of users whose logon information the computer will cache locally. If the number is set to 4, then the computer caches logon information for 4 users. When a 5th user logs on to the computer, the server overwrites the oldest cached logon session. Users who access the computer console will have their logon credentials cached on that computer. An attacker who is able to access the file system of the computer could locate this cached information and use a brute force attack to attempt to determine user passwords. To mitigate this type of attack, Windows encrypts the information and obscures its physical location.

CCE Reference Number: CCE-37439-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.7.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days' — Trivial

Vulnerability Details

This policy setting determines how far in advance users are warned that their password will expire. It is recommended that you configure this policy setting to at least 5 days but no more than 14 days to sufficiently warn users when their passwords will expire. The recommended state for this setting is: between 5 and 14 days .

Rationale: It is recommended that user passwords be configured to expire periodically. Users will need to be warned that their passwords are going to expire, or they may inadvertently be locked out of the computer when their passwords expire. This condition could lead to confusion for users who access the network locally, or make it impossible for users to access your organization's network through dial-up or virtual private network (VPN) connections.

CCE Reference Number: CCE-37622-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.7.7

Solution Details

To establish the recommended configuration via GP, set the following UI path to a value between 5 and 14 days: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration Impact: Users will see a dialog box prompt to change their password each time that they log on to the domain when their password is configured to expire between 5 and 14 days.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Prompt user to change password before expiration' is set to 'between 5 and 14 days'

Trivial

Vulnerability Details

This policy setting determines how far in advance users are warned that their password will expire. It is recommended that you configure this policy setting to at least 5 days but no more than 14 days to sufficiently warn users when their passwords will expire. The recommended state for this setting is: between 5 and 14 days.

Rationale: It is recommended that user passwords be configured to expire periodically. Users will need to be warned that their passwords are going to expire, or they may inadvertently be locked out of the computer when their passwords expire. This condition could lead to confusion for users who access the network locally, or make it impossible for users to access your organization's network through dial-up or virtual private network (VPN) connections.

CCE Reference Number: CCE-37622-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.7.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to a value between 5 and 14 days:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Prompt user to change password before expiration>

Impact: Users will see a dialog box prompt to change their password each time that they log on to the domain when their password is configured to expire between 5 and 14 days.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only) — Trivial

Solution Details

To implement the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Require Domain Controller Authentication to unlock workstation Impact: When the console on a computer is locked, either by a user or automatically by a screen saver time-out, the console can only be unlocked if the user is able to re-authenticate to the domain controller. If no domain controller is available, then users cannot unlock their workstations. If you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to 0, users whose domain controllers are unavailable (such as mobile or remote users) will not be able to log on.

Vulnerability Details

Logon information is required to unlock a locked computer. For domain accounts, the Interactive logon: Require Domain Controller authentication to unlock workstation setting determines whether it is necessary to contact a domain controller to unlock a computer. If you enable this setting, a domain controller must authenticate the domain account that is being used to unlock the computer. If you disable this setting, logon information confirmation with a domain controller is not required for a user to unlock the computer. However, if you configure the Interactive logon: Number of previous logons to cache (in case domain controller is not available) setting to a value that is greater than zero, then the user's cached credentials will be used to unlock the computer. The recommended state for this setting is: Enabled.

Rationale: By default, the computer caches in memory the credentials of any users who are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. When cached credentials are used, any changes that have recently been made to the account#x2014;such as user rights assignments, account lockout, or the account being disabled#x2014;are not considered or applied after the account is authenticated. User privileges are not updated, and (more importantly) disabled accounts are still able to unlock the console of the computer.

CCE Reference Number: CCE-38240-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.7.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Require Domain Controller Authentication to unlock workstation' is set to 'Enabled' (MS only)

Trivial

Solution Details

To implement the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Require Domain Controller Authentication to unlock workstation>

Impact: When the console on a computer is locked, either by a user or automatically by a screen saver time-out, the console can only be unlocked if a domain controller is available to re-authenticate the domain account that is being used to unlock the computer. If no domain controller is available, the user cannot unlock the computer.

Vulnerability Details

Logon information is required to unlock a locked computer. For domain accounts, the Interactive logon: Require Domain Controller authentication to unlock workstation setting determines whether it is necessary to contact a domain controller to unlock a computer. The recommended state for this setting is: Enabled.

Rationale: By default, the computer caches in memory the credentials of any users who are authenticated locally. The computer uses these cached credentials to authenticate anyone who attempts to unlock the console. When cached credentials are used, any changes that have recently been made to the account such as user rights assignments, account lockout, or the account being disabled are not considered or applied after the account is authenticated. User privileges are not updated, and (more importantly) disabled accounts are still able to unlock the console of the computer.

CCE Reference Number: CCE-38240-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.7.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher

Trivial

Vulnerability Details

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: Lock Workstation. Configuring this setting to Force Logoff or Disconnect if a Remote Desktop Services session also conforms with the benchmark.

Rationale: Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

CCE Reference Number: CCE-38333-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.7.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Lock Workstation (or, if applicable for your environment, Force Logoff or Disconnect if a Remote Desktop Services session): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior Impact: If you select Force Logoff, users will have to re-insert their smart cards and re-enter their PINs when they return to their workstations. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity.

For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Interactive logon: Smart card removal behavior' is set to 'Lock Workstation' or higher	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Lock Workstation (or, if applicable for your environment, Force Logoff or Disconnect if a Remote Desktop Services session):

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Smart card removal behavior>

Impact: If you select Lock Workstation, the workstation is locked when the smart card is removed, allowing users to leave the area, take their smart card with them, and still maintain a protected session. If you select Force Logoff, users are automatically logged off when their smart card is removed. If you select Disconnect if a Remote Desktop Services session, removal of the smart card disconnects the session without logging the users off. This allows the user to insert the smart card and resume the session later, or at another smart card reader-equipped computer, without having to log on again. If the session is local, this policy will function identically to Lock Workstation. Enforcing this setting on computers used by people who must log onto multiple computers in order to perform their duties could be frustrating and lower productivity.

For example, if network administrators are limited to a single account but need to log into several computers simultaneously in order to effectively manage the network enforcing this setting will limit them to logging onto one computer at a time. For these reasons it is recommended that this setting only be enforced on workstations used for purposes commonly associated with typical users such as document creation and email.

Vulnerability Details

This policy setting determines what happens when the smart card for a logged-on user is removed from the smart card reader. The recommended state for this setting is: Lock Workstation. Configuring this setting to Force Logoff or Disconnect if a Remote Desktop Services session also conforms with the benchmark.

Rationale: Users sometimes forget to lock their workstations when they are away from them, allowing the possibility for malicious users to access their computers. If smart cards are used for authentication, the computer should automatically lock itself when the card is removed to ensure that only the user with the smart card is accessing resources using those credentials.

CCE Reference Number: CCE-38333-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.7.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Join Microsoft MAPS' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Defender\MAPS\Join Microsoft MAPS>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows you to join Microsoft MAPS. Microsoft MAPS is the online community that helps you choose how to respond to potential threats. The community also helps stop the spread of new malicious software infections. You can choose to send basic or additional information about detected software. Additional information helps Microsoft create new definitions and help it to protect your computer. Possible options are: (0x0) Disabled (default) (0x1) Basic membership (0x2) Advanced membership Basic membership will send basic information to Microsoft about software that has been detected including where the software came from the actions that you apply or that are applied automatically and whether the actions were successful. Advanced membership in addition to basic information will send more information to Microsoft about malicious software spyware and potentially unwanted software including the location of the software file names how the software operates and how it has impacted your computer. The recommended state for this setting is: Disabled.

Rationale: This information can include things like location of detected items on your computer if harmful software was removed. The information will be automatically collected and sent. In some instances personal information might unintentionally be sent to Microsoft. However Microsoft will not use this information to identify you or contact you.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.69.3.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only)	Trivial

Solution Details

In order to utilize LAPS, a minor Active Directory Schema update is required, and a Group Policy Client Side Extension (CSE) must be installed on each managed computer. When LAPS is installed, the file AdmPwd.dll must be present in the following location and registered in Windows (the LAPS AdmPwd GPO Extension / CSE installation does this for you): C:\Program Files\LAPS\CSE\AdmPwd.dll Impact: No impact. When installed and registered properly, AdmPwd.dll takes no action unless given appropriate GPO commands during Group Policy refresh. It is not a memory-resident agent or service. In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure LAPS AdmPwd GPO Extension / CSE is installed (MS only)	Trivial

Solution Details

In order to utilize LAPS, a minor Active Directory Schema update is required, and a Group Policy Client Side Extension (CSE) must be installed on each managed computer. When LAPS is installed, the file AdmPwd.dll must be present in the following location and registered in Windows (the LAPS AdmPwd GPO Extension / CSE installation does this for you): C:\Program Files\LAPS\CSE\AdmPwd.dll

Impact: No impact. When installed and registered properly, AdmPwd.dll takes no action unless given appropriate GPO commands during Group Policy refresh. It is not a memory-resident agent or service. In a disaster recovery scenario where Active Directory is not available, the local Administrator password will not be retrievable and a local password reset using a tool (such as Microsoft's Disaster and Recovery Toolset (DaRT) Recovery Image) may be necessary.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.2.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Let Windows apps *' is set to 'Enabled: Force Deny'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI paths to Enabled: Force Deny: Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access account information Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access call history Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access contacts Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access email Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access location Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access messaging Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access motion Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access the calendar Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access the camera Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access the microphone Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access trusted devices Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps control radios Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps sync with devices Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps make phone calls Computer Configuration\Policies\Administrative Templates\Windows Components\App Privacy\Let Windows apps access notifications

Note: These Group Policy paths do not exist by default. An updated Group Policy template (AppPrivacy.admx/adml) is required to configure all of them - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Impact: Windows apps will be restricted from accessing potentially sensitive information or resources, and employees in your organization will not be able to change it.

Vulnerability Details

These policy settings specify whether Windows apps can access personal data, resources or other applications. The following 15 settings are in scope:
Let Windows apps access account information
Let Windows apps access call history Let Windows apps access contacts
Let Windows apps access email
Let Windows apps access location
Let Windows apps access messaging

Let Windows apps access motion
Let Windows apps access the calendar
Let Windows apps access the camera
Let Windows apps access the microphone
Let Windows apps access trusted devices
Let Windows apps control radios
Let Windows apps sync with devices
Let Windows apps make phone calls
Let Windows apps access notifications
The recommended state for these settings is: Enabled: Force Deny

Rationale: In an enterprise environment where you want to maintain user privacy, Windows apps should not need or require access to personal data, resources or other applications.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.5.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators'

Trivial

Vulnerability Details

This policy setting allows users to dynamically load a new device driver on a system. An attacker could potentially use this capability to install malicious code that appears to be a device driver. This user right is required for users to add local printers or printer drivers in Windows Vista. The recommended state for this setting is: Administrators.

Rationale: Device drivers run as highly privileged code. A user who has the Load and unload device drivers user right could unintentionally install malicious code that masquerades as a device driver. Administrators should exercise greater care and install only drivers with verified digital signatures.

CCE Reference Number: CCE-36318-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.27

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers Impact: If you remove the Load and unload device drivers user right from the Print Operators group or other accounts you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks will not be negatively affected.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Load and unload device drivers' is set to 'Administrators' — Trivial

Vulnerability Details

This policy setting allows users to dynamically load a new device driver on a system. An attacker could potentially use this capability to install malicious code that appears to be a device driver. This user right is required for users to add local printers or printer drivers in Windows Vista. The recommended state for this setting is: Administrators.

Rationale: Device drivers run as highly privileged code. A user who has the Load and unload device drivers user right could unintentionally install malicious code that masquerades as a device driver. Administrators should exercise greater care and install only drivers with verified digital signatures.

CCE Reference Number: CCE-36318-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.27

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Load and unload device drivers>

Impact: If you remove the Load and unload device drivers user right from the Print Operators group or other accounts you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks will not be negatively affected.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Lock pages in memory' is set to 'No One' — Trivial

Vulnerability Details

This policy setting allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. If this user right is assigned, significant degradation of system performance can occur. The recommended state for this setting is: No One.

Rationale: Users with the Lock pages in memory user right could assign physical memory to several processes, which could leave little or no RAM for other processes and result in a DoS condition.

CCE Reference Number: CCE-36495-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.28

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory Impact: None. This is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Lock pages in memory' is set to 'No One' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Lock pages in memory>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. If this user right is assigned, significant degradation of system performance can occur. The recommended state for this setting is: No One.

Rationale: Users with the Lock pages in memory user right could assign physical memory to several processes, which could leave little or no RAM for other processes and result in a DoS condition.

CCE Reference Number: CCE-36495-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.28

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Log on as a batch job' is set to 'Administrators' (DC Only)

Trivial

Vulnerability Details

This policy setting allows accounts to log on using the task scheduler service. Because the task scheduler is often used for administrative purposes, it may be needed in enterprise environments. However, its use should be restricted in high security environments to prevent misuse of system resources or to prevent attackers from using the right to launch malicious code after gaining user level access to a computer. When configuring a user right in the SCM enter a comma delimited list of accounts. Accounts can be either local or located in Active Directory, they can be groups, users, or computers. The recommended state for this setting is: Administrators.

Rationale: The Log on as a batch job user right presents a low-risk vulnerability. For most organizations, the default settings are sufficient.

CCE Reference Number: CCE-38080-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.29

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Administrators:

<Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Log on as a batch job>

Impact: If you configure the Log on as a batch job setting through domain-based Group Policies, the computer will not be able to assign the user right to accounts that are used for scheduled jobs in the

Task Scheduler. If you install optional components such as ASP.NET or IIS, you might need to assign this user right to additional accounts that are required by those components. For example, IIS requires assignment of this user right to the IIS_WPG group and the IUSR_(ComputerName), ASPNET, and IWAM_(ComputerName) accounts. If this user right is not assigned to this group and these accounts, IIS will be unable to run some COM objects that are necessary for proper functionality.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0'	Trivial

Vulnerability Details

This policy setting defines how long a user can use their password before it expires. Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire. Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current. The recommended state for this setting is 60 or fewer days, but not 0.

Rationale: The longer a password exists the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring the Maximum password age setting to 0 so that users are never required to change their passwords is a major security risk because that allows a compromised password to be used by the malicious user for as long as the valid user is authorized access.

CCE Reference Number: CCE-37167-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 1.1.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to 60 or fewer days, but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age Impact: If the Maximum password age setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization, because users might write their passwords in an insecure location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows potential attackers more time in which to discover user passwords or to use compromised accounts.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Maximum password age' is set to '60 or fewer days, but not 0' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 60 or fewer days, but not 0:

<Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Maximum password age>

Impact: If the Maximum password age setting is too low, users are required to change their passwords very often. Such a configuration can reduce security in the organization, because users might write their passwords in an insecure location or lose them. If the value for this policy setting is too high, the level of security within an organization is reduced because it allows potential attackers more time in which to discover user passwords or to use compromised accounts.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting defines how long a user can use their password before it expires. Values for this policy setting range from 0 to 999 days. If you set the value to 0, the password will never expire. Because attackers can crack passwords, the more frequently you change the password the less opportunity an attacker has to use a cracked password. However, the lower this value is set, the higher the potential for an increase in calls to help desk support due to users having to change their password or forgetting which password is current. The recommended state for this setting is 60 or fewer days, but not 0.

Rationale: The longer a password exists the higher the likelihood that it will be compromised by a brute force attack, by an attacker gaining general knowledge about the user, or by the user sharing the password. Configuring the Maximum password age setting to 0 so that users are never required to change their passwords is a major security risk because that allows a compromised password to be used by the malicious user for as long as the valid user is authorized access.

CCE Reference Number: CCE-37167-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 1.1.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	Trivial

Vulnerability Details

This policy setting determines whether packet signing is required by the SMB client component. If you enable this policy setting, the Microsoft network client computer cannot communicate with a Microsoft network server unless that server agrees to sign SMB packets. In mixed environments with legacy client computers, set this option to Disabled because these computers will not be able to authenticate or gain access to domain controllers. However, you can use this policy setting in Windows 2000 or later environments.

Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: Enabled.

Rationale: Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

CCE Reference Number: CCE-36325-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.8.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network client: Digitally sign communications (always)' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (always)>

Impact: The Microsoft network client will not communicate with a Microsoft network server unless that server agrees to perform SMB packet signing. The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Vulnerability Details

This policy setting determines whether packet signing is required by the SMB client component. Note: When Windows Vista-based computers have this policy setting enabled and they connect to file or print shares on remote servers, it is important that the setting is synchronized with its companion setting, Microsoft network server: Digitally sign communications (always), on those servers. For more information about these settings, see the "Microsoft network client and server: Digitally sign communications (four related settings)" section in Chapter 5 of the Threats and Countermeasures guide. The recommended state for this setting is: Enabled.

Rationale: Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

CCE Reference Number: CCE-36325-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.8.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (if server agrees) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting determines whether the SMB client will attempt to negotiate SMB packet signing. The implementation of digital signing in Windows-based networks helps to prevent sessions from being hijacked. If you enable this policy setting, the Microsoft network client will use signing only if the server with which it communicates accepts digitally signed communication. Note: Enabling this policy setting on SMB clients on your network makes them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: Enabled.

Rationale: Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

CCE Reference Number: CCE-36269-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.8.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network client: Digitally sign communications (if server agrees)' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting determines whether the SMB client will attempt to negotiate SMB packet signing. Note: Enabling this policy setting on SMB clients on your network makes them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: Enabled.

Rationale: Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

CCE Reference Number: CCE-36269-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.8.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Digitally sign communications (if server agrees)>

Impact: None - this is the default behavior. The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to third-party SMB servers Impact: Some very old applications and operating systems such as MS-DOS, Windows for Workgroups 3.11, and Windows 95a may not be able to communicate with the servers in your organization by means of the SMB protocol.

Vulnerability Details

Disable this policy setting to prevent the SMB redirector from sending plaintext passwords during authentication to third-party SMB servers that do not support password encryption. It is recommended that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network. The recommended state for this setting is: Disabled.

Rationale: If you enable this policy setting, the server can transmit passwords in plaintext across the network to other computers that offer SMB services. These other computers may not use any of the SMB security mechanisms that are included with Windows Server 2003.

CCE Reference Number: CCE-37863-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.8.3

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network client: Send unencrypted password to third-party SMB servers' is set to 'Disabled'

Trivial

Vulnerability Details

This policy setting determines whether the SMB redirector will send plaintext passwords during authentication to third-party SMB servers that do not support password encryption. It is recommended that you disable this policy setting unless there is a strong business case to enable it. If this policy setting is enabled, unencrypted passwords will be allowed across the network. The recommended state for this setting is: Disabled.

Rationale: If you enable this policy setting, the server can transmit passwords in plaintext across the network to other computers that offer SMB services, which is a significant security risk. These other computers may not use any of the SMB security mechanisms that are included with Windows Server 2003.

CCE Reference Number: CCE-37863-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.8.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network client: Send unencrypted password to third-party SMB servers>

Impact: None - this is the default configuration. Some very old applications and operating systems such as MS-DOS, Windows for Workgroups 3.11, and Windows 95a may not be able to communicate with the servers in your organization by means of the SMB protocol.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0'	Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to 15 or fewer minute(s), but not 0: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session Impact: There will be little impact because SMB sessions will be re-established automatically if the client resumes activity.

Vulnerability Details

This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished. A value of 0 appears to allow sessions to persist indefinitely. The maximum value is 99999, which is over 69 days; in effect, this value disables the setting. The recommended state for this setting is: 15 or fewer minute(s), but not 0.

Rationale: Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive.

CCE Reference Number: CCE-38046-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.9.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network server: Amount of idle time required before suspending session' is set to '15 or fewer minute(s), but not 0'

Trivial

Vulnerability Details

This policy setting allows you to specify the amount of continuous idle time that must pass in an SMB session before the session is suspended because of inactivity. Administrators can use this policy setting to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished. A value of 0 appears to allow sessions to persist indefinitely. The maximum value is 99999, which is over 69 days; in effect, this value disables the setting. The recommended state for this setting is: 15 or fewer minute(s), but not 0.

Rationale: Each SMB session consumes server resources, and numerous null sessions will slow the server or possibly cause it to fail. An attacker could repeatedly establish SMB sessions until the server's SMB services become slow or unresponsive.

CCE Reference Number: CCE-38046-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.9.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to 15 or fewer minute(s), but not 0:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Amount of idle time required before suspending session>

Impact: There will be little impact because SMB sessions will be re-established automatically if the client resumes activity.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Vulnerability Details

This policy setting determines if the server side SMB service is required to perform SMB packet signing. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: Enabled.

Rationale: Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

CCE Reference Number: CCE-37864-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.9.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network server: Digitally sign communications (always)' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting determines whether packet signing is required by the SMB server component. Enable this policy setting in a mixed environment to prevent downstream clients from using the workstation as a network server. The recommended state for this setting is: Enabled.

Rationale: Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

CCE Reference Number: CCE-37864-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.9.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (always)>

Impact: The Microsoft network server will not communicate with a Microsoft network client unless that client agrees to perform SMB packet signing. The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees) Impact: The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Vulnerability Details

This policy setting determines if the server side SMB service is able to sign SMB packets if it is requested to do so by a client that attempts to establish a connection. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled.

Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: Enabled.

Rationale: Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

CCE Reference Number: CCE-35988-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.9.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network server: Digitally sign communications (if client agrees)' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Digitally sign communications (if client agrees)>

Impact: The Microsoft network server will negotiate SMB packet signing as requested by the client. That is, if packet signing has been enabled on the client, packet signing will be negotiated. The Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional and Windows Vista implementations of the SMB file and print sharing protocol support mutual authentication, which prevents session hijacking attacks and supports message authentication to prevent man-in-the-middle attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server. Implementation of SMB signing may negatively affect performance, because each packet needs to be signed and verified. If these settings are enabled on a server that is performing multiple roles, such as a small business server that is serving as a domain controller, file server, print server, and application server performance may be substantially slowed. Additionally, if you configure computers to ignore all unsigned SMB communications, older applications and operating systems will not be able to connect. However, if you completely disable all SMB signing, computers will be vulnerable to session hijacking attacks. When SMB signing policies are enabled on domain controllers running Windows Server 2003 and member computers running Windows Vista SP1 or Windows Server 2008 group policy processing will fail. A hotfix is available from Microsoft that resolves this issue; see Microsoft Knowledge Base article 950876 for more details: Group Policy settings are not applied on member computers that are running Windows Server 2008 or Windows Vista SP1 when certain SMB signing policies are enabled.

Vulnerability Details

This policy setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. If no signing request comes from the client, a connection will be allowed without a signature if the Microsoft network server: Digitally sign communications (always) setting is not enabled.

Note: Enable this policy setting on SMB clients on your network to make them fully effective for packet signing with all clients and servers in your environment. The recommended state for this setting is: Enabled.

Rationale: Session hijacking uses tools that allow attackers who have access to the same network as the client or server to interrupt, end, or steal a session in progress. Attackers can potentially intercept and modify unsigned SMB packets and then modify the traffic and forward it so that the server might perform undesirable actions. Alternatively, the attacker could pose as the server or client after legitimate authentication and gain unauthorized access to data. SMB is the resource sharing protocol that is supported by many Windows operating systems. It is the basis of NetBIOS and many other protocols. SMB signatures authenticate both users and the servers that host the data. If either side fails the authentication process, data transmission will not take place.

CCE Reference Number: CCE-35988-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.9.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire Impact: If logon hours are not used in your organization, this policy setting will have no impact. If logon hours are used, existing user sessions will be forcibly terminated when their logon hours expire.

Vulnerability Details

This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. It affects the SMB component. If you enable this policy setting, client sessions with the SMB service will be forcibly disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions will be maintained after the client's logon hours expire. If you enable this policy setting you should also enable Network security: Force logoff when logon hours expire. If your organization configures logon hours for users, this policy setting is necessary to ensure they are effective. The recommended state for this setting is: Enabled.

Rationale: If your organization configures logon hours for users, then it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

CCE Reference Number: CCE-37972-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.9.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Microsoft network server: Disconnect clients when logon hours expire' is set to 'Enabled'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Disconnect clients when logon hours expire>

Impact: None - this is the default configuration. If logon hours are not used in your organization, this policy setting will have no impact. If logon hours are used, existing user sessions will be forcibly terminated when their logon hours expire.

Vulnerability Details

This security setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable Network security: Force logoff when logon hours expire (Rule 2.3.11.6). If your organization configures logon hours for users, this policy setting is necessary to ensure they are effective. The recommended state for this setting is: Enabled.

Rationale: If your organization configures logon hours for users, then it makes sense to enable this policy setting. Otherwise, users who should not have access to network resources outside of their logon hours may actually be able to continue to use those resources with sessions that were established during allowed hours.

CCE Reference Number: CCE-37972-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.9.4

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher

Trivial

Vulnerability Details

This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. This security setting determines the level of validation a SMB server performs on the service principal name (SPN) provided by the SMB client when trying to establish a session to an SMB server. The recommended state for this setting is: Accept if provided by client. Configuring this setting to Required from client also conforms with the benchmark.

Rationale: The identity of a computer can be spoofed to gain unauthorized access to network resources.

CCE Reference Number: CCE-36170-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.9.5

Solution Details

To establish the recommended configuration via GP, set the following UI path to Accept if provided by client (configuring to Required from client also conforms with the benchmark): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Server SPN target name validation level Impact: All Windows operating systems support both a client-side SMB component and a server-side SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft network server: Server SPN target name validation level' is set to 'Accept if provided by client' or higher (MS only)

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Accept if provided by client (configuring to Required from client also conforms to the benchmark):

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Microsoft network server: Server SPN target name validation level>

Impact: All Windows operating systems support both a client-side SMB component and a server-side

SMB component. This setting affects the server SMB behavior, and its implementation should be carefully evaluated and tested to prevent disruptions to file and print serving capabilities. If configured to Accept if provided by client, the SMB server will accept and validate the SPN provided by the SMB client and allow a session to be established if it matches the SMB servers list of SPNs for itself. If the SPN does NOT match, the session request for that SMB client will be denied. If configured to Required from client, the SMB client MUST send a SPN name in session setup, and the SPN name provided MUST match the SMB server that is being requested to establish a connection. If no SPN is provided by client, or the SPN provided does not match, the session is denied.

Note: Since the release of the MS KB3161561 security patch, this setting can cause significant issues (such as replication problems, group policy editing issues and blue screen crashes) on domain controllers when used simultaneously with UNC path hardening (i.e. rule 18.4.14.1). CIS therefore recommends against deploying this setting on domain controllers.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting controls the level of validation a computer with shared folders or printers (the server) performs on the service principal name (SPN) that is provided by the client computer when it establishes a session using the server message block (SMB) protocol. The server message block (SMB) protocol provides the basis for file and print sharing and other networking operations, such as remote Windows administration. The SMB protocol supports validating the SMB server service principal name (SPN) within the authentication blob provided by a SMB client to prevent a class of attacks against SMB servers referred to as SMB relay attacks. This setting will affect both SMB1 and SMB2. The recommended state for this setting is: Accept if provided by client. Configuring this setting to Required from client also conforms to the benchmark.

Rationale: The identity of a computer can be spoofed to gain unauthorized access to network resources.

CCE Reference Number: CCE-36170-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.9.5

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider' is set to 'Disabled'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Microsoft Support Diagnostic Tool\Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider>

Impact: MSDT cannot run in support mode, and no data can be collected or sent to the support provider.

Vulnerability Details

This policy setting configures Microsoft Support Diagnostic Tool (MSDT) interactive communication with the support provider. MSDT gathers diagnostic data for analysis by support professionals. The recommended state for this setting is: Disabled.

Rationale: Due to privacy concerns, data should never be sent to any 3rd party since this data could contain sensitive information.

CCE Reference Number: CCE-38161-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.39.5.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Minimize the number of simultaneous connections to the Internet or a Windows Domain Impact: If this policy setting is enabled, when the computer has at least one active connection to the Internet, a new automatic connection attempt to the Internet is blocked. When the computer has at least one active connection to a Windows domain, a new automatic connection to the same Windows domain is also blocked. Additional manual connection attempts by users to the Internet or to a Windows domain are not blocked by this policy setting.

Vulnerability Details

This policy setting prevents computers from establishing multiple simultaneous connections to either the Internet or to a Windows domain. The recommended state for this setting is: Enabled.

Rationale: Blocking simultaneous connections can help prevent a user unknowingly allowing network traffic to flow between the Internet and the corporate network.

CCE Reference Number: CCE-38338-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.4.20.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Minimize the number of simultaneous connections to the Internet or a Windows Domain' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Minimize the number of simultaneous connections to the Internet or a Windows Domain>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting prevents computers from connecting to both a domain based network and a non-domain based network at the same time. The recommended state for this setting is: Enabled.

Rationale: Blocking simultaneous connections can help prevent a user unknowingly allowing network traffic to flow between the Internet and the corporate network.

CCE Reference Number: CCE-38338-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.21.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)'	Trivial

Vulnerability Details

This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: 1 or more day(s).

Rationale: Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

CCE Reference Number: CCE-37073-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 1.1.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to 1 or more day(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age Impact: If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Minimum password age' is set to '1 or more day(s)'

Trivial

Vulnerability Details

This policy setting determines the number of days that you must use a password before you can change it. The range of values for this policy setting is between 1 and 999 days. (You may also set the value to 0 to allow immediate password changes.) The default value for this setting is 0 days. The recommended state for this setting is: 1 or more day(s).

Rationale: Users may have favorite passwords that they like to use because they are easy to remember and they believe that their password choice is secure from compromise. Unfortunately, passwords are compromised and if an attacker is targeting a specific individual user account, with foreknowledge of data about that user, reuse of old passwords can cause a security breach. To address password reuse a combination of security settings is required. Using this policy setting with the Enforce password history setting prevents the easy reuse of old passwords. For example, if you configure the Enforce password history setting to ensure that users cannot reuse any of their last 12 passwords, they could change their password 13 times in a few minutes and reuse the password they started with, unless you also configure the Minimum password age setting to a number that is greater than 0. You must configure this policy setting to a number that is greater than 0 for the Enforce password history setting to be effective.

CCE Reference Number: CCE-37073-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 1.1.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to 1 or more day(s):

<Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password age>

Impact: If an administrator sets a password for a user but wants that user to change the password when the user first logs on, the administrator must select the User must change password at next logon check box, or the user will not be able to change the password until the next day.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 14 or more character(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length Impact: Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave the information in an insecure location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about pass phrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.

Note: Older versions of Windows such as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

Vulnerability Details

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 or later, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length.In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: 14 or more character(s).

Rationale: Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

CCE Reference Number: CCE-36534-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 1.1.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Minimum password length' is set to '14 or more character(s)'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 14 or more character(s):

<Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length>

Impact: Requirements for extremely long passwords can actually decrease the security of an organization, because users might leave the information in an insecure location or lose it. If very long passwords are required, mistyped passwords could cause account lockouts and increase the volume of help desk calls. If your organization has issues with forgotten passwords due to password length requirements, consider teaching your users about pass phrases, which are often easier to remember and, due to the larger number of character combinations, much harder to discover.

Note: Older versions of Windows such as Windows 98 and Windows NT 4.0 do not support passwords that are longer than 14 characters. Computers that run these older operating systems are unable to authenticate with computers or domains that use accounts that require long passwords.

Vulnerability Details

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps "pass phrase" is a better term than "password." In Microsoft Windows 2000 or later, pass phrases can be quite long and can include spaces. Therefore, a phrase such as "I want to drink a $5 milkshake" is a valid pass phrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: 14 or more character(s).

Rationale: Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

CCE Reference Number: CCE-36534-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 1.1.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Modify an object label' is set to 'No One' — Trivial

Vulnerability Details

This privilege determines which user accounts can modify the integrity label of objects, such as files, registry keys, or processes owned by other users. Processes running under a user account can modify the label of an object owned by that user to a lower level without this privilege. The recommended state for this setting is: No One.

Rationale: By modifying the integrity label of an object owned by another user a malicious user may cause them to execute code at a higher level of privilege than intended.

CCE Reference Number: CCE-36054-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.31

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label Impact: None, by default the Administrators group has this user right.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Modify an object label' is set to 'No One' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify an object label>

Impact: None - this is the default configuration.

Vulnerability Details

This privilege determines which user accounts can modify the integrity label of objects, such as files, registry keys, or processes owned by other users. Processes running under a user account can modify the label of an object owned by that user to a lower level without this privilege. The recommended state for this setting is: No One.

Rationale: By modifying the integrity label of an object owned by another user a malicious user may cause them to execute code at a higher level of privilege than intended.

CCE Reference Number: CCE-36054-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.31

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators'

Trivial

Vulnerability Details

This policy setting allows users to configure the system-wide environment variables that affect hardware configuration. This information is typically stored in the Last Known Good Configuration. Modification of these values and could lead to a hardware failure that would result in a denial of service condition. The recommended state for this setting is: Administrators.

Rationale: Anyone who is assigned the Modify firmware environment values user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition.

CCE Reference Number: CCE-38113-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.32

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values Impact: None. This is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Modify firmware environment values' is set to 'Administrators' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Modify firmware environment values>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows users to configure the system-wide environment variables that affect hardware configuration. This information is typically stored in the Last Known Good Configuration. Modification of these values and could lead to a hardware failure that would result in a denial of service condition. The recommended state for this setting is: Administrators.

Rationale: Anyone who is assigned the Modify firmware environment values user right could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition.

CCE Reference Number: CCE-38113-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.32

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).
Impact: None. By default this entry is not enabled.

Vulnerability Details

This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group. For additional information, see Microsoft Knowledge Base article 324737: How to turn on automatic logon in Windows. The recommended state for this setting is: Disabled.

Rationale: If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

CCE Reference Number: CCE-37067-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.3.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)' is set to 'Disabled'	Trivial

Vulnerability Details

This setting is separate from the Welcome screen feature in Windows XP and Windows Vista; if that feature is disabled, this setting is not disabled. If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks to which the computer is connected. Also, if you enable automatic logon, the password is stored in the registry in plaintext, and the specific registry key that stores this value is remotely readable by the Authenticated Users group. For additional information, see Microsoft Knowledge Base article 324737: How to turn on automatic logon in Windows. The recommended state for this setting is: Disabled.

Rationale: If you configure a computer for automatic logon, anyone who can physically gain access to the computer can also gain access to everything that is on the computer, including any network or networks that the computer is connected to. Also, if you enable automatic logon, the password is stored in the registry in plaintext. The specific registry key that stores this setting is remotely readable by the Authenticated Users group. As a result, this entry is appropriate only if the computer is physically secured and if you ensure that untrusted users cannot remotely see the registry.

CCE Reference Number: CCE-37067-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disa...

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).

Impact: All incoming source routed packets will be dropped.

Vulnerability Details

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled.

Rationale: An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

CCE Reference Number: CCE-36535-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.3.3

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely disabled'	Trivial

Vulnerability Details

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should take through the network. It is recommended to configure this setting to Not Defined for enterprise environments and to Highest Protection for high security environments to completely disable source routing. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled.

Rationale: An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

CCE Reference Number: CCE-36535-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: All incoming source routed packets will be dropped.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely...

Trivial

Vulnerability Details

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled.

Rationale: An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

CCE Reference Number: CCE-36871-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.3.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled: Computer Configuration\Policies\Administrative

Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).
Impact: All incoming source routed packets will be dropped.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)' is set to 'Enabled: Highest protection, source routing is completely ...	Trivial

Vulnerability Details

IP source routing is a mechanism that allows the sender to determine the IP route that a datagram should follow through the network. The recommended state for this setting is: Enabled: Highest protection, source routing is completely disabled.

Rationale: An attacker could use source routed packets to obscure their identity and location. Source routing allows a computer that sends a packet to specify the route that the packet takes.

CCE Reference Number: CCE-36871-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Highest protection, source routing is completely disabled:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: All incoming source routed packets will be dropped.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled : Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).

Impact: When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Vulnerability Details

Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes. The recommended state for this setting is: Disabled.

Rationale: This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

CCE Reference Number: CCE-37988-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.3.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: When Routing and Remote Access Service (RRAS) is configured as an autonomous system boundary router (ASBR), it does not correctly import connected interface subnet routes. Instead, this router injects host routes into the OSPF routes. However, the OSPF router cannot be used as an ASBR router, and when connected interface subnet routes are imported into OSPF the result is confusing routing tables with strange routing paths.

Vulnerability Details

Internet Control Message Protocol (ICMP) redirects cause the IPv4 stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) generated routes. The recommended state for this setting is: Disabled.

Rationale: This behavior is expected. The problem is that the 10 minute time-out period for the ICMP redirect-plumbed routes temporarily creates a network situation in which traffic will no longer be routed properly for the affected host. Ignoring such ICMP redirects will limit the system's exposure to attacks that will impact its ability to participate on the network.

CCE Reference Number: CCE-37988-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Type	Reference

Compliance: Ensure 'MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds' is set to 'Enabled: 300,000 or 5 minutes (recommended)'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 300,000 or 5 minutes (recommended):

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: Keep-alive packets are not sent by default by Windows. However, some applications may configure the TCP stack flag that requests keep-alive packets. For such configurations, you can lower this value from the default setting of two hours to five minutes to disconnect inactive sessions more quickly.

Vulnerability Details

This value controls how often TCP attempts to verify that an idle connection is still intact by sending a keep-alive packet. If the remote computer is still reachable, it acknowledges the keep-alive packet. The recommended state for this setting is: Enabled: 300,000 or 5 minutes (recommended).

Rationale: An attacker who is able to connect to network applications could establish numerous connections to cause a DoS condition.

CCE Reference Number: CCE-36868-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM). Impact: An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment.

Vulnerability Details

NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request. The recommended state for this setting is: Enabled.

Rationale: The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries. The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

CCE Reference Number: CCE-36879-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.3.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: None - this is the default configuration.

Vulnerability Details

NetBIOS over TCP/IP is a network protocol that among other things provides a way to easily resolve NetBIOS names that are registered on Windows-based systems to the IP addresses that are configured on those systems. This setting determines whether the computer releases its NetBIOS name when it receives a name-release request. The recommended state for this setting is: Enabled.

Rationale: The NetBT protocol is designed not to use authentication, and is therefore vulnerable to spoofing. Spoofing makes a transmission appear to come from a user other than the user who performed the action. A malicious user could exploit the unauthenticated nature of the protocol to send a name-conflict datagram to a target computer, which would cause the computer to relinquish its name and not respond to queries. An attacker could send a request over the network and query a computer to release its NetBIOS name. As with any change that could affect applications, it is recommended that you test this change in a non-production environment before you change the production environment. The result of such an attack could be to cause intermittent connectivity issues on the target computer, or even to prevent the use of Network Neighborhood, domain logons, the NET SEND command, or additional NetBIOS name resolution.

CCE Reference Number: CCE-36879-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)' is set to 'Disabled'	**Trivial**

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: Windows will not automatically detect and configure default gateway addresses on the computer.

Vulnerability Details

This setting is used to enable or disable the Internet Router Discovery Protocol (IRDP), which allows the system to detect and configure default gateway addresses automatically as described in RFC 1256 on a per-interface basis. The recommended state for this setting is: Disabled.

Rationale: An attacker who has gained control of a computer on the same network segment could configure a computer on the network to impersonate a router. Other computers with IRDP enabled would then attempt to route their traffic through the already compromised computer.

CCE Reference Number: CCE-38065-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).

Impact: Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems.

Vulnerability Details

The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways: Search folders specified in the system path first, and then search the current working folder. Search current working folder first, and then search the folders specified in the system path. When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path. The recommended state for this setting is: Enabled.

Rationale: If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

CCE Reference Number: CCE-36351-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.3.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: None - this is the default configuration.

Vulnerability Details

The DLL search order can be configured to search for DLLs that are requested by running processes in one of two ways: Search folders specified in the system path first, and then search the current working folder. Search current working folder first, and then search the folders specified in the system path. When enabled, the registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path and then searches the current working folder. When disabled the registry value is set to 0 and the system first searches the current working folder and then searches the folders that are specified in the system path. Applications will be forced to search for DLLs in the system path first. For applications that require unique versions of these DLLs that are included with the application, this entry could cause performance or stability problems. The recommended state for this setting is: Enabled.

Rationale: If a user unknowingly executes hostile code that was packaged with additional files that include modified versions of system DLLs, the hostile code could load its own versions of those DLLs and potentially increase the type and degree of damage the code can render.

CCE Reference Number: CCE-36351-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 5 or fewer seconds: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).

Impact: Users will have to enter their passwords to resume their console sessions as soon as the screen saver activates.

Vulnerability Details

Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled. The recommended state for this setting is: Enabled: 5 or fewer seconds.

Rationale: The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

CCE Reference Number: CCE-37993-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.3.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)' is set to 'Enabled: 5 or fewer seconds'

Trivial

Vulnerability Details

Windows includes a grace period between when the screen saver is launched and when the console is actually locked automatically when screen saver locking is enabled. The recommended state for this setting is: Enabled: 5 or fewer seconds.

Rationale: The default grace period that is allowed for user movement before the screen saver lock takes effect is five seconds. If you leave the default grace period configuration, your computer is vulnerable to a potential attack from someone who could approach the console and attempt to log on to the computer before the lock takes effect. An entry to the registry can be made to adjust the length of the grace period.

CCE Reference Number: CCE-37993-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.9

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 5 or fewer seconds:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: Users will have to enter their passwords to resume their console sessions as soon as the grace period ends after screen saver activation.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 3:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

Vulnerability Details

This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection. The recommended state for this setting is: Enabled: 3.

Rationale: A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

CCE Reference Number: CCE-36051-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.11

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted' is set to 'Enabled: 3'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 3:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: TCP starts a retransmission timer when each outbound segment is passed to the IP. If no acknowledgment is received for the data in a given segment before the timer expires, then the segment is retransmitted up to three times.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This setting controls the number of times that TCP retransmits an individual data segment (non-connect segment) before the connection is aborted. The retransmission time-out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time-out value is dynamically determined by the measured round-trip time on the connection. The recommended state for this setting is: Enabled: 3.

Rationale: A malicious user could exhaust a target computer's resources if it never sent any acknowledgment messages for data that was transmitted by the target computer.

CCE Reference Number: CCE-37846-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.10

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	**Trivial**

Vulnerability Details

This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold.

Note: If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated. The recommended state for this setting is: Enabled: 90% or less.

Rationale: If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

CCE Reference Number: CCE-36880-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.3.12

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 90% or less: Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning

Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).

Impact: This setting will generate an audit event when the Security log reaches the 90 percent-full threshold unless the log is configured to overwrite events as needed.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning' is set to 'Enabled: 90% or less'	Trivial

Vulnerability Details

This setting can generate a security audit in the Security event log when the log reaches a user-defined threshold. Note: If log settings are configured to Overwrite events as needed or Overwrite events older than x days, this event will not be generated. The recommended state for this setting is: Enabled: 90% or less.

Rationale: If the Security log reaches 90 percent of its capacity and the computer has not been configured to overwrite events as needed, more recent events will not be written to the log. If the log reaches its capacity and the computer has been configured to shut down when it can no longer record events to the Security log, the computer will shut down and will no longer be available to provide network services.

CCE Reference Number: CCE-36880-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.3.12

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 90% or less:

<Computer Configuration\Policies\Administrative Templates\MSS (Legacy)\MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning Note: This Group Policy path does not exist by default. An additional Group Policy template (MSS-legacy.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM), or available from this TechNet blog post: https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/>

Impact: An audit event will be generated when the Security log reaches the 90% percent full threshold (or whatever lower value may be set) unless the log is configured to overwrite events as needed.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation Impact: Disabled is the default configuration for this policy setting on member computers; therefore it will have no impact on them. The default configuration for domain controllers is Enabled. If you disable this policy setting on domain controllers, legacy computers may be unable to communicate with Windows Server 2003-based domains. For example, the following computers may not work: Windows NT 4.0-based Remote Access Service servers. Microsoft SQL Servers#x2122; that run on Windows NT 3.x-based or Windows NT 4.0-based computers. Remote Access Service or Microsoft SQL servers that run on Windows 2000-based computers and are located in Windows NT 3.x domains or Windows NT 4.0 domains.

Vulnerability Details

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. Disable this policy setting to prevent unauthenticated users from obtaining user names that are associated with their respective SIDs. The recommended state for this setting is: Disabled.

Rationale: If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

CCE Reference Number: CCE-36065-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.10.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Allow anonymous SID/Name translation' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines whether an anonymous user can request security identifier (SID) attributes for another user, or use a SID to obtain its corresponding user name. The recommended state for this setting is: Disabled.

Rationale: If this policy setting is enabled, a user with local access could use the well-known Administrator's SID to learn the real name of the built-in Administrator account, even if it has been renamed. That person could then use the account name to initiate a password guessing attack.

CCE Reference Number: CCE-36065-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Allow anonymous SID/Name translation>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled'	Trivial

Vulnerability Details

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the workstations in your environment.

The Network access: Do not allow anonymous enumeration of SAM accounts and shares setting is configured to Enabled for the two environments that are discussed in this guide. The recommended state for this setting is: Enabled.

Rationale: An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks.

CCE Reference Number: CCE-36077-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.10.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares Impact: It will be impossible to grant access to users of another domain across a one-way trust because administrators in the trusting domain will be unable to enumerate lists of accounts in the other domain. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts and shares' is set to 'Enabled' (MS only)	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts and shares>

Impact: It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server. Users who access file and print servers anonymously will be unable to list the shared network resources on those servers; the users will have to authenticate before they can view the lists of shared folders and printers. However, even with this policy setting enabled, anonymous users will have access to resources with permissions that explicitly include the built-in group, ANONYMOUS LOGON.

Vulnerability Details

This policy setting controls the ability of anonymous users to enumerate SAM accounts as well as shares. If you enable this policy setting, anonymous users will not be able to enumerate domain account user names and network share names on the systems in your environment. The recommended state for this setting is: Enabled.

Note: This policy has no effect on domain controllers.

Rationale: An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

CCE Reference Number: CCE-36077-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections cannot enumerate domain account user names on the workstations in your environment. This policy setting also allows additional restrictions on anonymous connections. The recommended state for this setting is: Enabled.

Rationale: An unauthorized user could anonymously list account names and use the information to perform social engineering attacks or attempt to guess passwords. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

CCE Reference Number: CCE-36316-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.10.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts Impact: It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Do not allow anonymous enumeration of SAM accounts' is set to 'Enabled' (MS only)	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow anonymous enumeration of SAM accounts>

Impact: None - this is the default configuration. It will be impossible to establish trusts with Windows NT 4.0-based domains. Also, client computers that run older versions of the Windows operating system such as Windows NT 3.51 and Windows 95 will experience problems when they try to use resources on the server.

Vulnerability Details

This policy setting controls the ability of anonymous users to enumerate the accounts in the Security Accounts Manager (SAM). If you enable this policy setting, users with anonymous connections will not be able to enumerate domain account user names on the systems in your environment. This policy setting also allows additional restrictions on anonymous connections. The recommended state for this setting is: Enabled.

Note: This policy has no effect on domain controllers.

Rationale: An unauthorized user could anonymously list account names and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.)

CCE Reference Number: CCE-36316-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Do not allow storage of passwords and credentials for network authentication' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Do not allow storage of passwords and credentials for network authentication>

Impact: Credential Manager will not store passwords and credentials on the computer. Users will be forced to enter passwords whenever they log on to their Passport account or other network resources that aren't accessible to their domain account. Testing has shown that clients running Windows Vista or Windows Server 2008 will be unable to connect to Distributed File System (DFS) shares in untrusted domains. Enabling this setting also makes it impossible to specify alternate credentials for scheduled tasks, this can cause a variety of problems. For example, some third party backup products will no longer work. This policy setting should have no impact on users who access network resources that are configured to allow access with their Active Directory-based domain account.

Vulnerability Details

This policy setting determines whether Credential Manager (formerly called Stored User Names and Passwords) saves passwords or credentials for later use when it gains domain authentication. The recommended state for this setting is: Enabled.

Note: Changes to this setting will not take effect until Windows is restarted.

Rationale: Passwords that are cached can be accessed by the user when logged on to the computer. Although this information may sound obvious, a problem can arise if the user unknowingly executes hostile code that reads the passwords and forwards them to another, unauthorized user.

CCE Reference Number: CCE-38119-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines what additional permissions are assigned for anonymous connections to the computer. If you enable this policy setting, anonymous Windows users are allowed to perform certain activities, such as enumerate the names of domain accounts and network shares. An unauthorized user could anonymously list account names and shared resources and use the information to guess passwords or perform social engineering attacks. The recommended state for this setting is: Disabled.

Rationale: An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords, perform social engineering attacks, or launch DoS attacks.

CCE Reference Number: CCE-36148-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.10.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users Impact: None. This is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Let Everyone permissions apply to anonymous users' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines what additional permissions are assigned for anonymous connections to the computer. The recommended state for this setting is: Disabled.

Rationale: An unauthorized user could anonymously list account names and shared resources and use the information to attempt to guess passwords, perform social engineering attacks, or launch DoS attacks.

CCE Reference Number: CCE-36148-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Let Everyone permissions apply to anonymous users>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Remotely accessible registry paths'

Trivial

Vulnerability Details

This policy setting determines which registry paths will be accessible after referencing the WinReg key to determine access permissions to the paths. Note: This setting does not exist in Windows XP. There was a setting with that name in Windows XP, but it is called "Network access: Remotely accessible registry paths and sub-paths" in Windows Server 2003, Windows Vista, and Windows Server 2008. Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. The recommended state for this setting is: System\CurrentControlSet\Control\ProductOptionsSystem\CurrentControlSet\Control\Server ApplicationsSoftware\Microsoft\Windows NT\CurrentVersion

Rationale: The registry is a database that contains computer configuration information, and much of the information is sensitive. An attacker could use this information to facilitate unauthorized activities. To reduce the risk of such an attack, suitable ACLs are assigned throughout the registry to help protect it from access by unauthorized users.

CCE Reference Number: CCE-37194-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.10.7

Solution Details

To establish the recommended configuration via GP, set the following UI path to: System\CurrentControlSet\Control\ProductOptionsSystem\CurrentControlSet\Control\Server ApplicationsSoftware\Microsoft\Windows NT\CurrentVersion Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths Impact: Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail.

Note: If you want to allow remote access, you must also enable the Remote Registry service.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Remotely accessible registry paths and sub-paths'

Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to: System\CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\Services\EventlogSoftwar ServerSoftware\Microsoft\Windows NT\CurrentVersion\PrintSoftware\Microsoft\Windows NT\CurrentVersion\WindowsSystem\CurrentControlSet\Control\ContentIndexSystem\CurrentControlS ServerSystem\CurrentControlSet\Control\Terminal Server\UserConfigSystem\CurrentControlSet\Control\Terminal Server\DefaultUserConfigurationSoftware\Microsoft\Windows NT\CurrentVersion\PerflibSystem\CurrentControlSet\Services\SysmonLog

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Remotely accessible registry paths and sub-paths When a server holds the Active Directory Certificate Services Role with Certification Authority Role Service, the above list should

also include: System\CurrentControlSet\Services\CertSvc. When a server has the WINS Server Feature installed, the above list should also include: System\CurrentControlSet\Services\WINS>

Impact: Remote management tools such as the Microsoft Baseline Security Analyzer and Microsoft Systems Management Server require remote access to the registry to properly monitor and manage those computers. If you remove the default registry paths from the list of accessible ones, such remote management tools could fail. Note: If you want to allow remote access, you must also enable the Remote Registry service.

Vulnerability Details

This policy setting determines which registry paths and sub-paths will be accessible when an application or process references the WinReg key to determine access permissions. Note: In Windows XP this setting is called "Network access: Remotely accessible registry paths," the setting with that same name in Windows Vista, Windows Server 2008, and Windows Server 2003 does not exist in Windows XP. Note #2: When you configure this setting you specify a list of one or more objects. The delimiter used when entering the list is a line feed or carriage return, that is, type the first object on the list, press the Enter button, type the next object, press Enter again, etc. The setting value is stored as a comma-delimited list in group policy security templates. It is also rendered as a comma-delimited list in Group Policy Editor's display pane and the Resultant Set of Policy console. It is recorded in the registry as a line-feed delimited list in a REG_MULTI_SZ value. The recommended state for this setting is:

System\CurrentControlSet\Control\Print\PrintersSystem\CurrentControlSet\Services\EventlogSoftwar
ServerSoftware\Microsoft\Windows NT\CurrentVersion\PrintSoftware\Microsoft\Windows
NT\CurrentVersion\WindowsSystem\CurrentControlSet\Control\ContentIndexSystem\CurrentControlS
ServerSystem\CurrentControlSet\Control\Terminal
Server\UserConfigSystem\CurrentControlSet\Control\Terminal
Server\DefaultUserConfigurationSoftware\Microsoft\Windows
NT\CurrentVersion\PerflibSystem\CurrentControlSet\Services\SysmonLog

The recommended state for servers that hold the Active Directory Certificate Services Role with Certification Authority Role Service includes the above list and: System\CurrentControlSet\Services\CertSvc The recommended state for servers that have the WINS Server Feature installed includes the above list and: System\CurrentControlSet\Services\WINS

Rationale: The registry contains sensitive computer configuration information that could be used by an attacker to facilitate unauthorized activities. The fact that the default ACLs assigned throughout the registry are fairly restrictive and help to protect the registry from access by unauthorized users reduces the risk of such an attack.

CCE Reference Number: CCE-36347-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.10.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named Pipes and Shares Impact: You can enable this policy setting to restrict null session access for unauthenticated users to all server pipes and shared folders except those that are listed in the NullSessionPipes and NullSessionShares entries. If you choose to enable this setting and are supporting Windows NT 4.0 domains, you should check if any of the named pipes are required to maintain trust relationships between the domains, and then add the pipe to the Network access: Named pipes that can be accessed anonymously list:- COMNAP: SNA session access- COMNODE: SNA session access- SQL\QUERY: SQL instance access- SPOOLSS: Spooler service- LLSRPC: License Logging service- NETLOGON: Net Logon service- LSARPC: LSA access- SAMR: Remote access to SAM objects- BROWSER: Computer Browser service Previous to the release of Windows Server 2003 with Service Pack 1 (SP1) these named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 these pipes must be explicitly added if needed.

Vulnerability Details

When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the Network access: Named pipes that can be accessed anonymously and Network access: Shares that can be accessed anonymously settings. This policy setting controls null session access to shares on your computers by adding RestrictNullSessAccess with the value 1 in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters registry key. This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources. The recommended state for this setting is: Enabled.

Rationale: Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

CCE Reference Number: CCE-36021-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.10.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Network access: Restrict anonymous access to Named Pipes and Shares' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict anonymous access to Named Pipes and Shares>

Impact: None - this is the default configuration. If you choose to enable this setting and are supporting Windows NT 4.0 domains, you should check if any of the named pipes are required to maintain trust relationships between the domains, and then add the pipe to the Network access: Named pipes that can be accessed anonymously list: - COMNAP: SNA session access - COMNODE: SNA session access - SQL\QUERY: SQL instance access - SPOOLSS: Spooler service - LLSRPC: License Logging service - NETLOGON: Net Logon service - LSARPC: LSA access - SAMR: Remote access to SAM objects - BROWSER: Computer Browser service Previous to the release of Windows Server 2003 with Service Pack 1 (SP1) these named pipes were allowed anonymous access by default, but with the increased hardening in Windows Server 2003 with SP1 these pipes must be explicitly added if needed.

Vulnerability Details

When enabled, this policy setting restricts anonymous access to only those shares and pipes that are named in the Network access: Named pipes that can be accessed anonymously and Network access: Shares that can be accessed anonymously settings.

This policy setting controls null session access to shares on your computers by adding RestrictNullSessAccess with the value 1 in the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters registry key.

This registry value toggles null session shares on or off to control whether the server service restricts unauthenticated clients' access to named resources. The recommended state for this setting is: Enabled.

Rationale: Null sessions are a weakness that can be exploited through shares (including the default shares) on computers in your environment.

CCE Reference Number: CCE-36021-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Restrict clients allowed to make remote calls to SAM' is set to 'Administrators: Remote Access: Allow' (MS only)	Trivial

Vulnerability Details

This policy setting allows you to restrict remote RPC connections to SAM. The recommended state for this setting is: Administrators: Remote Access: Allow.

Note: A Windows 10 R1607, Server 2016 or higher OS is required to access and set this value in Group Policy.

Rationale: To ensure that an unauthorized user cannot anonymously list local account names or groups and use the information to attempt to guess passwords or perform social engineering attacks. (Social engineering attacks try to deceive users in some way to obtain passwords or some form of security information.) CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.10

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Remote Access: Allow:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Restrict clients allowed to make remote calls to SAM>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None'	Trivial

Vulnerability Details

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server. The recommended state for this setting is: <blank> (i.e. None).

Rationale: It is very dangerous to enable this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

CCE Reference Number: CCE-38095-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.10.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to <blank> (i.e. None): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously Impact: There should be little impact because this is the default configuration. Only authenticated users will have access to shared resources on the server.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Shares that can be accessed anonymously' is set to 'None' — Trivial

Vulnerability Details

This policy setting determines which network shares can be accessed by anonymous users. The default configuration for this policy setting has little effect because all users have to be authenticated before they can access shared resources on the server. The recommended state for this setting is: <blank> (i.e. None).

Rationale: It is very dangerous to allow any values in this setting. Any shares that are listed can be accessed by any network user, which could lead to the exposure or corruption of sensitive data.

CCE Reference Number: CCE-38095-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.11

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to <blank> (i.e. None):

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Shares that can be accessed anonymously>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'

Trivial

Vulnerability Details

This policy setting determines how network logons that use local accounts are authenticated. The Classic option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The Guest only option allows you to treat all users equally. In this context, all users authenticate as Guest only to receive the same access level to a given resource. The recommended state for this setting is: Classic - local users authenticate as themselves.

Rationale: With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

CCE Reference Number: CCE-37623-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.10.11

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Classic - local users authenticate as themselves: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts Impact: None. This is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network access: Sharing and security model for local accounts' is set to 'Classic - local users authenticate as themselves'

Trivial

Vulnerability Details

This policy setting determines how network logons that use local accounts are authenticated. The Classic option allows precise control over access to resources, including the ability to assign different types of access to different users for the same resource. The Guest only option allows you to treat all users equally. In this context, all users authenticate as Guest only to receive the same access level to a given resource. The recommended state for this setting is: Classic - local users authenticate as themselves.

Note: This setting does not affect interactive logons that are performed remotely by using such services as Telnet or Remote Desktop Services (formerly called Terminal Services).

Rationale: With the Guest only model, any user who can authenticate to your computer over the network does so with guest privileges, which probably means that they will not have write access to shared resources on that computer. Although this restriction does increase security, it makes it more difficult for authorized users to access shared resources on those computers because ACLs on those resources must include access control entries (ACEs) for the Guest account. With the Classic model, local accounts should be password protected. Otherwise, if Guest access is enabled, anyone can use those user accounts to access shared system resources.

CCE Reference Number: CCE-37623-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.10.12

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Classic - local users authenticate as themselves:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network access: Sharing and security model for local accounts>

Impact: None - this is the default configuration for domain-joined computers.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow LocalSystem NULL session fallback Impact: Any applications that require NULL sessions for LocalSystem will not work as designed.

Vulnerability Details

Allow NTLM to fall back to NULL session when used with LocalSystem. The default is TRUE up to Windows Vista / Server 2008 and FALSE from Windows 7 / Server 2008 R2 and beyond. The recommended state for this setting is: Disabled.

Rationale: NULL sessions are less secure because by definition they are unauthenticated.

CCE Reference Number: CCE-37035-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Allow LocalSystem NULL session fallback' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security

Options\Network security: Allow LocalSystem NULL session fallback>

Impact: Any applications that require NULL sessions for LocalSystem will not work as designed.

Vulnerability Details

This policy setting determines whether NTLM is allowed to fall back to a NULL session when used with LocalSystem. The recommended state for this setting is: Disabled.

Rationale: NULL sessions are less secure because by definition they are unauthenticated.

CCE Reference Number: CCE-37035-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM Impact: If you enable this policy setting, services running as Local System that use Negotiate will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error. If you disable this policy setting, services running as Local System that use Negotiate when reverting to NTLM authentication will authenticate anonymously. This was the behavior in previous versions of Windows.

Vulnerability Details

When enabled, this policy setting causes Local System services that use Negotiate to use the computer identity when NTLM authentication is selected by the negotiation. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: Enabled.

Rationale: When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008, services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

CCE Reference Number: CCE-38341-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Allow Local System to use computer identity for NTLM' is set to 'Enabled' — Trivial

Vulnerability Details

This policy setting determines whether Local System services that use Negotiate when reverting to NTLM authentication can use the computer identity. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: Enabled.

Rationale: When connecting to computers running versions of Windows earlier than Windows Vista or Windows Server 2008, services running as Local System and using SPNEGO (Negotiate) that revert to NTLM use the computer identity. In Windows 7, if you are connecting to a computer running Windows Server 2008 or Windows Vista, then a system service uses either the computer identity or a NULL session. When connecting with a NULL session, a system-generated session key is created, which provides no protection but allows applications to sign and encrypt data without errors. When connecting with the computer identity, both signing and encryption is supported in order to provide data protection.

CCE Reference Number: CCE-38341-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Allow Local System to use computer identity for NTLM>

Impact: Services running as Local System that use Negotiate when reverting to NTLM authentication will use the computer identity. This might cause some authentication requests between Windows operating systems to fail and log an error.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled'	Trivial

Vulnerability Details

This setting determines if online identities are able to authenticate to this computer. Windows 7 and Windows Server 2008 R2 introduced an extension to the Negotiate authentication package, Spnego.dll. In previous versions of Windows, Negotiate decides whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, Negoexts, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U. When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes. The recommended state for this setting is: Disabled.

Rationale: The PKU2U protocol is a peer-to-peer authentication protocol, in most managed networks authentication should be managed centrally.

CCE Reference Number: CCE-38047-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities Impact: Disabling this setting will disallow the online identities to be able to authenticate to the domain joined machine in Windows 7 and later.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Network Security: Allow PKU2U authentication requests to this computer to use online identities' is set to 'Disabled' | Trivial

Vulnerability Details

This setting determines if online identities are able to authenticate to this computer. The Public Key Cryptography Based User-to-User (PKU2U) protocol introduced in Windows 7 and Windows Server 2008 R2 is implemented as a security support provider (SSP). The SSP enables peer-to-peer authentication, particularly through the Windows 7 media and file sharing feature called Homegroup, which permits sharing between computers that are not members of a domain. With PKU2U, a new extension was introduced to the Negotiate authentication package, Spnego.dll. In previous versions of Windows, Negotiate decided whether to use Kerberos or NTLM for authentication. The extension SSP for Negotiate, Negoexts.dll, which is treated as an authentication protocol by Windows, supports Microsoft SSPs including PKU2U. When computers are configured to accept authentication requests by using online IDs, Negoexts.dll calls the PKU2U SSP on the computer that is used to log on. The PKU2U SSP obtains a local certificate and exchanges the policy between the peer computers. When validated on the peer computer, the certificate within the metadata is sent to the logon peer for validation and associates the user's certificate to a security token and the logon process completes. The recommended state for this setting is: Disabled.

Rationale: The PKU2U protocol is a peer-to-peer authentication protocol - authentication should be managed centrally in most managed networks.

CCE Reference Number: CCE-38047-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Allow PKU2U authentication requests to this computer to use online identities>

Impact: None - this is the default configuration for domain-joined computers.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Configure encryption types allowed for Kerberos>

Impact: None - this is the default configuration. If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted. Note: Windows Server 2008 (non-R2) and below allow DES for Kerberos by default, but later OS versions do not.

Vulnerability Details

This policy setting allows you to set the encryption types that Kerberos is allowed to use. The recommended state for this setting is: RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types.

Rationale: The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

CCE Reference Number: CCE-37755-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network Security: Configure encryption types allowed for Kerberos' is set to 'RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network Security: Configure encryption types allowed for Kerberos Impact: If not selected, the encryption type will not be allowed. This setting may affect compatibility with client computers or services and applications. Multiple selections are permitted.

Vulnerability Details

This policy setting allows you to set the encryption types that Kerberos is allowed to use. This policy is supported on at least Windows 7 or Windows Server 2008 R2. The recommended state for this setting is: RC4_HMAC_MD5, AES128_HMAC_SHA1, AES256_HMAC_SHA1, Future encryption types.

Rationale: The strength of each encryption algorithm varies from one to the next, choosing stronger algorithms will reduce the risk of compromise however doing so may cause issues when the computer attempts to authenticate with systems that do not support them.

CCE Reference Number: CCE-37755-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change Impact: Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications will fail.

Vulnerability Details

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Microsoft Windows NT hash. Note: Older operating systems and some third-party applications may fail when this policy setting is enabled. Also, note that the password will need to be changed on all accounts after you enable this setting to gain the proper benefit. The recommended state for this setting is: Enabled.

Rationale: The SAM file can be targeted by attackers who seek access to username and password hashes. Such attacks use special tools to crack passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks will not be prevented if you enable this policy setting, but it will be much more difficult for these types of attacks to succeed.

CCE Reference Number: CCE-36326-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Do not store LAN Manager hash value on next password change' is set to 'Enabled'	Trivial

Vulnerability Details

This policy setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack compared to the cryptographically stronger Microsoft Windows NT hash. Since LM hashes are stored on the local computer in the security database, passwords can then be easily compromised if the database is attacked.

Note: Older operating systems and some third-party applications may fail when this policy setting is enabled. Also, note that the password will need to be changed on all accounts after you enable this setting to gain the proper benefit. The recommended state for this setting is: Enabled.

Rationale: The SAM file can be targeted by attackers who seek access to username and password hashes. Such attacks use special tools to crack passwords, which can then be used to impersonate users and gain access to resources on your network. These types of attacks will not be prevented if you enable this policy setting, but it will be much more difficult for these types of attacks to succeed.

CCE Reference Number: CCE-36326-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.5

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Do not store LAN Manager hash value on next password change>

Impact: None - this is the default configuration. Earlier operating systems such as Windows 95, Windows 98, and Windows ME as well as some third-party applications will fail.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled'	Trivial

Vulnerability Details

This policy setting, which determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours, affects the SMB component. If you enable this policy setting, client sessions with the SMB server will be disconnected when the client's logon hours expire. If you disable this policy setting, established client sessions will be maintained after the client's logon hours expire. The recommended state for this setting is: Enabled.

Rationale: If this setting is disabled, a user could remain connected to the computer outside of their allotted logon hours.

CCE Reference Number: CCE-36270-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.6

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled. Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Force logoff when logon hours expire Impact: When a user's logon time expires, SMB sessions will terminate. The user will be unable to log on to the computer until their next scheduled access time commences.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Force logoff when logon hours expire' is set to 'Enabled' — Trivial

Vulnerability Details

This policy setting determines whether to disconnect users who are connected to the local computer outside their user account's valid logon hours. This setting affects the Server Message Block (SMB) component. If you enable this policy setting you should also enable Microsoft network server: Disconnect clients when logon hours expire (Rule 2.3.9.4). The recommended state for this setting is: Enabled.

Rationale: If this setting is disabled, a user could remain connected to the computer outside of their allotted logon hours.

CCE Reference Number: CCE-36270-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled.

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Force logoff when logon hours expire>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM & NTLM' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to: Send NTLMv2 response only. Refuse LM & NTLM: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level Impact: Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM. Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see Microsoft Knowledge Base article 305379: Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain.

Vulnerability Details

LAN Manager (LM) is a family of early Microsoft client/server software that allows users to link personal computers together on a single network. Network capabilities include transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations: Join a domain Authenticate between Active Directory forests Authenticate to down-level domains Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP) Authenticate to computers that are not in the domain The possible values for the Network security: LAN Manager authentication level setting are: Send LM & NTLM responses Send LM & NTLM #x2014; use NTLMv2 session security if negotiated Send NTLM responses only Send NTLMv2 responses only Send NTLMv2 responses only\refuse LM Send NTLMv2 responses only\refuse LM & NTLM Not Defined The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the authentication protocol level that clients use, the session security level that the computers negotiate, and the authentication level that servers accept as follows: Send LM & NTLM responses. Clients use LM and NTLM authentication and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. Send LM & NTLM - use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. Send NTLM response only. Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. Send NTLMv2 response only. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. Send NTLMv2 response only\refuse LM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM (accept only NTLM and NTLMv2 authentication). Send NTLMv2 response only\refuse LM & NTLM. Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. Domain controllers refuse LM and NTLM (accept only NTLMv2 authentication). These settings correspond to the levels discussed in other Microsoft documents as follows: Level 0 - Send LM and NTLM response; never use NTLMv2 session security. Clients use LM and NTLM authentication, and never use NTLMv2 session security. Domain controllers accept LM, NTLM, and NTLMv2 authentication. Level 1 - Use NTLMv2 session security if negotiated. Clients use LM and NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. Level 2 - Send NTLM response only. Clients use only NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. Level 3 - Send NTLMv2 response only. Clients use NTLMv2 authentication, and use NTLMv2 session security if the server supports it. Domain controllers accept LM, NTLM, and NTLMv2 authentication. Level 4 - Domain controllers refuse LM responses. Clients use NTLM authentication, and use NTLMv2 session security if the server supports it. Domain controllers refuse LM authentication, that is, they accept NTLM and NTLMv2. Level 5 - Domain controllers refuse LM and NTLM responses (accept only NTLMv2). Clients use NTLMv2 authentication, use and NTLMv2 session security if the server supports it. Domain controllers refuse NTLM and LM authentication (they accept only NTLMv2). The recommended state for this setting is: Send NTLMv2 response only. Refuse LM & NTLM.

Rationale: In Windows Vista, this setting is undefined. However, in Windows 2000, Windows Server 2003, and Windows XP clients are configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default setting on servers allows all clients to authenticate with servers and use their resources. However, this means that LM responses#x2014;the weakest form of authentication response#x2014;are sent over the network, and it is potentially possible for attackers to sniff that traffic to more easily reproduce the user's password. The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for earlier clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 domain controllers.

CCE Reference Number: CCE-36173-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: LAN Manager authentication level' is set to 'Send NTLMv2 response only. Refuse LM&NTLM'

Trivial

Vulnerability Details

LAN Manager (LM) was a family of early Microsoft client/server software (predating Windows NT) that allowed users to link personal computers together on a single network. LM network capabilities included transparent file and print sharing, user security features, and network administration tools. In Active Directory domains, the Kerberos protocol is the default authentication protocol. However, if the Kerberos protocol is not negotiated for some reason, Active Directory will use LM, NTLM, or NTLMv2. LAN Manager authentication includes the LM, NTLM, and NTLM version 2 (NTLMv2) variants, and is the protocol that is used to authenticate all Windows clients when they perform the following operations:

Join a domain Authenticate between Active Directory forests Authenticate to down-level domains Authenticate to computers that do not run Windows 2000, Windows Server 2003, or Windows XP Authenticate to computers that are not in the domain. The Network security: LAN Manager authentication level setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of session security negotiated, and the level of authentication accepted by servers. The recommended state for this setting is: Send NTLMv2 response only. Refuse LM & NTLM.

Rationale: Windows 2000 and Windows XP clients were configured by default to send LM and NTLM authentication responses (Windows 95-based and Windows 98-based clients only send LM). The default settings in OSes predating Windows Vista / Windows Server 2008 (non-R2) allowed all clients to authenticate with servers and use their resources. However, this meant that LM responses - the weakest form of authentication response - were sent over the network, and it was potentially possible for attackers to sniff that traffic to more easily reproduce the user's password. The Windows 95, Windows 98, and Windows NT operating systems cannot use the Kerberos version 5 protocol for authentication. For this reason, in a Windows Server 2003 domain, these computers authenticate by default with both the LM and NTLM protocols for network authentication. You can enforce a more secure authentication protocol for Windows 95, Windows 98, and Windows NT by using NTLMv2. For the logon process, NTLMv2 uses a secure channel to protect the authentication process. Even if you use NTLMv2 for earlier clients and servers, Windows-based clients and servers that are members of the domain will use the Kerberos authentication protocol to authenticate with Windows Server 2003 or higher domain controllers. For these reasons, it is strongly preferred to restrict the use of LM & NTLM (non-v2) as much as possible.

CCE Reference Number: CCE-36173-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.7

Solution Details

To establish the recommended configuration via GP, set the following UI path to: Send NTLMv2 response only. Refuse LM & NTLM:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LAN Manager authentication level>

Impact: Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it; domain controllers refuse LM and NTLM (accept only NTLMv2 authentication). Clients that do not support NTLMv2 authentication will not be able to authenticate in the domain and access domain resources by using LM and NTLM. Note: For information about a hotfix to ensure that this setting works in networks that include Windows NT 4.0-based computers along with Windows 2000, Windows XP, and Windows Server 2003-based computers, see Microsoft Knowledge Base article 305379: Authentication Problems in Windows 2000 with NTLM 2 Levels Above 2 in a Windows NT 4.0 Domain.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher	Trivial

Vulnerability Details

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests, as follows:- None. The LDAP BIND request is issued with the caller-specified options.- Negotiate signing. If Transport Layer Security/Secure Sockets Layer (TLS/SSL) has not been started, the LDAP BIND request is initiated with the LDAP data signing option set in addition to the caller-specified options. If TLS/SSL has been started, the LDAP BIND request is initiated with the caller-specified options.- Require signature. This level is the same as Negotiate signing. However, if the LDAP server's intermediate saslBindInProgress response does not indicate that LDAP traffic signing is required, the caller is told that the LDAP BIND command request failed. Note: This policy setting does not have any impact on ldap_simple_bind or ldap_simple_bind_s. No Microsoft LDAP clients that are included with Windows XP Professional use ldap_simple_bind or ldap_simple_bind_s to communicate with a domain controller. The possible values for the Network security: LDAP client signing requirements setting are:- None- Negotiate signing- Require signature- Not Defined The recommended state for this setting is: Negotiate signing. Configuring this setting to Require signing also conforms with the benchmark.

Rationale: Unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures the packets between the client and server, modifies them, and then forwards them to the server. For an LDAP server, this susceptibility means that an attacker could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk in your network, you can implement strong physical security measures to protect the network infrastructure. Also, you can make all types of man-in-the-middle attacks extremely difficult if you require digital signatures on all network packets by means of IPsec authentication headers.

CCE Reference Number: CCE-36858-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.8

Solution Details

To establish the recommended configuration via GP, set the following UI path to Negotiate signing (configuring to Require signing also conforms with the benchmark): Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LDAP client signing requirements Impact: If you configure the server to require LDAP signatures you must also configure the client. If you do not configure the client it will not be able to communicate with the server, which could cause many features to fail, including user authentication, Group Policy, and logon scripts.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: LDAP client signing requirements' is set to 'Negotiate signing' or higher

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Negotiate signing(configuring to Require signing also conforms with the benchmark):

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: LDAP client signing requirements>

Impact: None - this is the default configuration. However, if you choose instead to configure the server to require LDAP signatures then you must also configure the client. If you do not configure the client it will not be able to communicate with the server, which could cause many features to fail, including user authentication, Group Policy, and logon scripts, because the caller will be told that the LDAP BIND command request failed.

Vulnerability Details

This policy setting determines the level of data signing that is requested on behalf of clients that issue LDAP BIND requests. Note: This policy setting does not have any impact on LDAP simple bind (ldap_simple_bind) or LDAP simple bind through SSL (ldap_simple_bind_s). No Microsoft LDAP clients that are included with Windows XP Professional use ldap_simple_bind or ldap_simple_bind_s to communicate with a domain controller. The recommended state for this setting is: Negotiate signing. Configuring this setting to Require signing also conforms with the benchmark.

Rationale: Unsigned network traffic is susceptible to man-in-the-middle attacks in which an intruder captures the packets between the client and server, modifies them, and then forwards them to the server. For an LDAP server, this susceptibility means that an attacker could cause a server to make decisions that are based on false or altered data from the LDAP queries. To lower this risk in your network, you can implement strong physical security measures to protect the network infrastructure. Also, you can make all types of man-in-the-middle attacks extremely difficult if you require digital signatures on all network packets by means of IPsec authentication headers.

CCE Reference Number: CCE-36858-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients Impact: Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Vulnerability Details

This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) clients setting are:- Requires message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption.

Rationale: You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

CCE Reference Number: CCE-37553-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) clients' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Require NTLMv2 session security, Require 128-bit encryption:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) clients>

Impact: NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not both negotiated. Client applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Vulnerability Details

This policy setting determines which behaviors are allowed by clients for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Note: These values are dependent on the Network security: LAN Manager Authentication Level security setting value.

Rationale: You can enable both options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. In other words, these options help protect against man-in-the-middle attacks.

CCE Reference Number: CCE-37553-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'	**Trivial**

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Require NTLMv2 session security, Require 128-bit encryption: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers

Impact: Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Vulnerability Details

This policy setting determines which behaviors are allowed for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The possible values for the Network security: Minimum session security for NTLM SSP based (including secure RPC) servers setting are:- Require message confidentiality. This option is only available in Windows XP and Windows Server 2003, the connection will fail if encryption is not negotiated. Encryption converts data into a form that is not readable until decrypted.- Require message integrity. This option is only available in Windows XP and Windows Server 2003, the connection will fail if message integrity is not negotiated. The integrity of a message can be assessed through message signing. Message signing proves that the message has not been tampered with; it attaches a cryptographic signature that identifies the sender and is a numeric representation of the contents of the message.- Require 128-bit encryption. The connection will fail if strong encryption (128-bit) is not negotiated.- Require NTLMv2 session security. The connection will fail if the NTLMv2 protocol is not negotiated.- Not Defined. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption.

Rationale: You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

CCE Reference Number: CCE-37835-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.11.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Network security: Minimum session security for NTLM SSP based (including secure RPC) servers' is set to 'Require NTLMv2 session security, Require 128-bit encryption'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Require NTLMv2 session security, Require 128-bit encryption:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Minimum session security for NTLM SSP based (including secure RPC) servers>

Impact: NTLM connections will fail if NTLMv2 protocol and strong encryption (128-bit) are not both negotiated. Server applications that are enforcing these settings will be unable to communicate with older servers that do not support them. This setting could impact Windows Clustering when applied to servers running Windows Server 2003, see Microsoft Knowledge Base articles 891597: How to apply more restrictive security settings on a Windows Server 2003-based cluster server and 890761: You receive an "Error 0x8007042b" error message when you add or join a node to a cluster if you use NTLM version 2 in Windows Server 2003 for more information on possible issues and how to resolve them.

Vulnerability Details

This policy setting determines which behaviors are allowed by servers for applications using the NTLM Security Support Provider (SSP). The SSP Interface (SSPI) is used by applications that need authentication services. The setting does not modify how the authentication sequence works but instead require certain behaviors in applications that use the SSPI. The recommended state for this setting is: Require NTLMv2 session security, Require 128-bit encryption. Note: These values are dependent on the Network security: LAN Manager Authentication Level security setting value.

Rationale: You can enable all of the options for this policy setting to help protect network traffic that uses the NTLM Security Support Provider (NTLM SSP) from being exposed or tampered with by an attacker who has gained access to the same network. That is, these options help protect against man-in-the-middle attacks.

CCE Reference Number: CCE-37835-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.11.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\No auto-restart with logged on users for scheduled automatic updates installations Impact: If you enable this policy setting, the operating systems on the servers in your environment will restart themselves automatically. For critical servers this could lead to a temporary denial of service (DoS) condition.

Vulnerability Details

This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation. If you enable the No auto-restart for scheduled Automatic Updates installations setting, Automatic Updates does not restart computers automatically during scheduled installations. Instead, Automatic Updates notifies users to restart their computers to complete the installations. You should note that Automatic Updates will not be able to detect future updates until restarts occur on the affected computers. If you disable or do not configure this setting, Automatic Updates will notify users that their computers will automatically restart in 5 minutes to complete the installations. The possible values for the No auto-restart for scheduled Automatic Updates installations setting are:- Enabled- Disabled- Not Configured

Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect. The recommended state for this setting is: Disabled.

Rationale: Sometimes updates require updated computers to be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted.

CCE Reference Number: CCE-37027-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.85.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'No auto-restart with logged on users for scheduled automatic updates installations' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\No auto-restart with logged on users for scheduled automatic updates installations>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting specifies that Automatic Updates will wait for computers to be restarted by the users who are logged on to them to complete a scheduled installation. The recommended state for this setting is: Disabled.

Note: This setting applies only when you configure Automatic Updates to perform scheduled update installations. If you configure the Configure Automatic Updates setting to Disabled, this setting has no effect.

Rationale: Sometimes updates require updated computers to be restarted to complete an installation. If the computer cannot restart automatically, then the most recent update will not completely install and no new updates will download to the computer until it is restarted.

CCE Reference Number: CCE-37027-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.90.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Notify antivirus programs when opening attachments' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\Notify antivirus programs when opening attachments Impact: When the Notify antivirus programs when opening attachments setting is Enabled, every downloaded file or e-mail attachment that the user opens will be scanned.

Vulnerability Details

Antivirus programs are mandatory in many environments and provide a strong defense against attack. The Notify antivirus programs when opening attachments setting allows you to manage how registered antivirus programs are notified. When enabled, this policy setting configures Windows to call the registered antivirus program and have it scan file attachments when they are opened by users. If the antivirus scan fails, the attachments are blocked from being opened. If this policy setting is disabled, Windows does not call the registered antivirus program when file attachments are opened. The recommended state for this setting is: Enabled. Note: An updated antivirus program must be installed for this policy setting to function properly.

Rationale: Antivirus programs that do not perform on-access checks may not be able to scan downloaded files.

CCE Reference Number: CCE-36622-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 19.7.4.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements Impact: If the default password complexity configuration is retained, additional help desk calls for locked-out accounts could occur because users might not be accustomed to passwords that contain non-alphabetic characters. However, all users should be able to comply with the complexity requirement with minimal difficulty. If your organization has more stringent security requirements, you can create a custom version of the Passfilt.dll file that allows the use of arbitrarily complex password strength rules.

For example, a custom password filter might require the use of non-upper row characters. (Upper row characters are those that require you to hold down the SHIFT key and press any of the digits between 1 and 0.) A custom password filter might also perform a dictionary check to verify that the proposed password does not contain common dictionary words or fragments. Also, the use of ALT key character combinations can greatly enhance the complexity of a password. However, such stringent password requirements can result in unhappy users and an extremely busy help desk. Alternatively, your organization could consider a requirement for all administrator passwords to use ALT characters in the 01280159 range. (ALT characters outside of this range can represent standard alphanumeric characters that would not add additional complexity to the password.)

Vulnerability Details

This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords. When this policy is enabled, passwords must meet the following minimum requirements:- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters- Be at least six characters in length- Contain characters from three of the following four categories:- English uppercase characters (A through Z)- English lowercase characters (a through z)- Base 10 digits (0 through 9)- Non-alphabetic characters (for example, !, $, #, %)- A catch-all category of any Unicode character that does not fall under the previous four categories. This fifth category can be regionally specific. Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 267 (approximately 8 x 109 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 527 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 268 (or 2 x 1011) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack. The recommended state for this setting is: Enabled.

Rationale: Passwords that contain only alphanumeric characters are extremely easy to discover with several publicly available tools.

CCE Reference Number: CCE-37063-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 1.1.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Password must meet complexity requirements' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Password must meet complexity requirements>

Impact: If the default password complexity configuration is retained, additional help desk calls for locked-out accounts could occur because users might not be accustomed to passwords that contain non-alphabetic characters. However, all users should be able to comply with the complexity requirement with minimal difficulty. If your organization has more stringent security requirements, you can create a custom version of the Passfilt.dll file that allows the use of arbitrarily complex password strength rules. For example, a custom password filter might require the use of non-upper row characters. (Upper row characters are those that require you to hold down the SHIFT key and press any of the digits between 1 and 0.) A custom password filter might also perform a dictionary check to verify that the proposed password does not contain common dictionary words or fragments. Also, the use of ALT key character combinations can greatly enhance the complexity of a password. However, such stringent password requirements can result in unhappy users and an extremely busy help desk. Alternatively, your organization could consider a requirement for all administrator passwords to use ALT characters in the 01280159 range. (ALT characters outside of this range can represent standard alphanumeric characters that would not add additional complexity to the password.)

Vulnerability Details

This policy setting checks all new passwords to ensure that they meet basic requirements for strong passwords. When this policy is enabled, passwords must meet the following minimum requirements: - Not contain the user's account name or parts of the user's full name that exceed two consecutive characters - Be at least six characters in length - Contain characters from three of the following four categories: - English uppercase characters (A through Z) - English lowercase characters (a through z) - Base 10 digits (0 through 9) - Non-alphabetic characters (for example, !, $, #, %) - A catch-all category of any Unicode character that does not fall under the previous four categories. This fifth category can be regionally specific. Each additional character in a password increases its complexity exponentially. For instance, a seven-character, all lower-case alphabetic password would have 267 (approximately 8 x 109 or 8 billion) possible combinations. At 1,000,000 attempts per second (a capability of many password-cracking utilities), it would only take 133 minutes to crack. A seven-character alphabetic password with case sensitivity has 527 combinations. A seven-character case-sensitive alphanumeric password without punctuation has 627 combinations. An eight-character password has 268 (or 2 x 1011) possible combinations. Although this might seem to be a large number, at 1,000,000 attempts per second it would take only 59 hours to try all possible passwords. Remember, these times will significantly increase for passwords that use ALT characters and other special keyboard characters such as "!" or "@". Proper use of the password settings can help make it difficult to mount a brute force attack. The recommended state for this setting is: Enabled.

Rationale: Passwords that contain only alphanumeric characters are extremely easy to discover with several publicly available tools.

CCE Reference Number: CCE-37063-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 1.1.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Password protect the screen saver' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Password protect the screen saver Impact: Users will have to provide their logon credentials when they want to access their locked desktop session.

Vulnerability Details

If the Password protect the screen saver setting is enabled, then all screen savers are password protected, if it is disabled then password protection cannot be set on any screen saver. The recommended state for this setting is: Enabled.

Rationale: If a user forgets to lock their computer when they walk away it is possible that a passerby will hijack it.

CCE Reference Number: CCE-37658-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 19.1.3.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only) — Trivial

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: 30 or fewer.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.2.6

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Age (Days) option to 30 or fewer: Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: Requires a maximum password age of 30 days or less.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Password Settings: Password Age (Days)' is set to 'Enabled: 30 or fewer' (MS only)	Trivial

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: 30 or fewer. Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.2.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Age (Days) option to 30 or fewer: Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact: LAPS-generated passwords will be required to have a maximum age of 30 days (or fewer, if selected).

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only)	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Complexity option to Large letters + small letters + numbers + special characters: Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact: Requires password to contain large letters + small letters + numbers + special characters

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: Large letters + small letters + numbers + special characters.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account.

CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.2.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Password Settings: Password Complexity' is set to 'Enabled: Large letters + small letters + numbers + special characters' (MS only)	Trivial

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: Large letters + small letters + numbers + special characters.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.2.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Complexity option to Large letters + small letters + numbers + special characters: Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS). Impact: LAPS-generated passwords will be required to contain large letters + small letters + numbers + special characters.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only) — Trivial

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: 15 or more.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.2.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Length option to 15 or more: Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact: Requires the password to have a length of a minimum of 15 characters .

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Password Settings: Password Length' is set to 'Enabled: 15 or more' (MS only)	Trivial

Vulnerability Details

In May 2015, Microsoft released the Local Administrator Password Solution (LAPS) tool, which is free and supported software that allows an organization to automatically set randomized and unique local Administrator account passwords on domain-attached workstations and member servers. The passwords are stored in a confidential attribute of the domain computer account and can be retrieved from Active Directory by approved Sysadmins when needed. The LAPS tool requires a small Active Directory Schema update in order to implement, as well as installation of a Group Policy Client Side Extension (CSE) on targeted computers. Please see the LAPS documentation for details. LAPS supports Windows Vista or newer workstation OSes, and Server 2003 or newer server OSes. LAPS does not support standalone computers - they must be joined to a domain. The recommended state for this setting is: Enabled: 15 or more.

Note: Organizations that utilize 3rd-party commercial software to manage unique & complex local Administrator passwords on domain members may opt to disregard these LAPS recommendations.

Rationale: Due to the difficulty in managing local Administrator passwords, many organizations choose to use the same password on all workstations and/or member servers when deploying them. This poses a serious attack surface security risk because if an attacker manages to compromise one system and learn the password to its local Administrator account, then they can leverage that account to instantly gain access to all other computers that also use that password for their local Administrator account. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.2.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled, and configure the Password Length option to 15 or more: Computer Configuration\Policies\Administrative Templates\LAPS\Password Settings

Note: This Group Policy path does not exist by default. An additional Group Policy template (AdmPwd.admx/adml) is required - it is included with Microsoft Local Administrator Password Solution (LAPS).

Impact: LAPS-generated passwords will be required to have a length of 15 characters (or more, if selected).

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' — Trivial

Vulnerability Details

This policy setting allows users to manage the system's volume or disk configuration, which could allow a user to delete a volume and cause data loss as well as a denial-of-service condition. The recommended state for this setting is: Administrators.

Rationale: A user who is assigned the Perform volume maintenance tasks user right could delete a volume, which could result in the loss of data or a DoS condition.

CCE Reference Number: CCE-36143-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.33

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Perform volume maintenance tasks Impact: None. This is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Perform volume maintenance tasks' is set to 'Administrators' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights

Assignment\Perform volume maintenance tasks>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting allows users to manage the system's volume or disk configuration, which could allow a user to delete a volume and cause data loss as well as a denial-of-service condition. The recommended state for this setting is: Administrators.

Rationale: A user who is assigned the Perform volume maintenance tasks user right could delete a volume, which could result in the loss of data or a DoS condition.

CCE Reference Number: CCE-36143-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.33

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent access to the about:flags page in Microsoft Edge' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting lets you decide whether employees can access the about:flags page, which is used to change developer settings and to enable experimental features. The recommended state for this setting is: Enabled.

Rationale: Users should not have access to access developer settings and experimental features, vulnerabilities could be introduced if not properly managed.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft

Edge\Prevent access to the about:flags page in Microsoft Edge>

Impact: Employees will not be able to access the about:flags page.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent bypassing SmartScreen prompts for files' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Prevent bypassing SmartScreen prompts for files>

Impact: Employees will not be able to ignore SmartScreen Filter warnings on files, and they will be blocked from downloading unverified files (that are potentially malicious) that SmartScreen detects.

Vulnerability Details

This setting lets you decide whether employees can override the SmartScreen Filter warnings about downloading unverified files. The recommended state for this setting is: Enabled.

Rationale: SmartScreen will warn an employee if a file is potentially malicious. Enabling this setting prevents these warnings from being bypassed.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent bypassing SmartScreen prompts for sites' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Prevent bypassing SmartScreen prompts for sites>

Impact: Employees will not be able to ignore SmartScreen Filter warnings, and they will be blocked from going to potentially malicious websites that SmartScreen detects.

Vulnerability Details

This setting lets you decide whether employees can override the SmartScreen Filter warnings about potentially malicious websites. The recommended state for this setting is: Enabled.

Rationale: SmartScreen will warn an employee if a website is potentially malicious. Enabling this setting prevents these warnings from being bypassed.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures Impact: If you disable or do not configure this policy setting, the user can set the Feed Sync Engine to download an enclosure through the Feed property page. A developer can change the download setting through the Feed APIs.

Vulnerability Details

This policy setting prevents the user from having enclosures (file attachments) downloaded from a feed to the user's computer. The recommended state for this setting is: Enabled.

Rationale: Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

CCE Reference Number: CCE-37126-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.49.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Prevent downloading of enclosures' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\Prevent downloading of enclosures>

Impact: Users cannot set the Feed Sync Engine to download an enclosure through the Feed property page. Developers cannot change the download setting through feed APIs.

Vulnerability Details

This policy setting prevents the user from having enclosures (file attachments) downloaded from a feed to the user's computer. The recommended state for this setting is: Enabled.

Rationale: Allowing attachments to be downloaded through the RSS feed can introduce files that could have malicious intent.

CCE Reference Number: CCE-37126-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.53.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' — Trivial

Vulnerability Details

Disables the lock screen camera toggle switch in PC Settings and prevents a camera from being invoked on the lock screen. The recommended state for this setting is: Enabled.

Rationale: Disabling the lock screen camera extends the protection afforded by the lock screen to camera features.

CCE Reference Number: CCE-38347-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.1.1.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen camera Impact: If you enable this setting, users will no longer be able to enable or disable lock screen camera access in PC Settings, and the camera cannot be invoked on the lock screen.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent enabling lock screen camera' is set to 'Enabled' — Trivial

Vulnerability Details

Disables the lock screen camera toggle switch in PC Settings and prevents a camera from being invoked on the lock screen. The recommended state for this setting is: Enabled.

Rationale: Disabling the lock screen camera extends the protection afforded by the lock screen to camera features.

CCE Reference Number: CCE-38347-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.1.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen camera>

Impact: If you enable this setting, users will no longer be able to enable or disable lock screen camera access in PC Settings, and the camera cannot be invoked on the lock screen.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen slide show Impact: If you enable this setting, users will no longer be able to modify slide show settings in PC Settings, and no slide show will ever start.

Vulnerability Details

Disables the lock screen slide show settings in PC Settings and prevents a slide show from playing on the lock screen. The recommended state for this setting is: Enabled.

Rationale: Disabling the lock screen slide show extends the protection afforded by the lock screen to slide show contents.

CCE Reference Number: CCE-38348-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.1.1.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent enabling lock screen slide show' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization\Prevent enabling lock screen slide show>

Impact: If you enable this setting, users will no longer be able to modify slide show settings in PC Settings, and no slide show will ever start.

Vulnerability Details

Disables the lock screen slide show settings in PC Settings and prevents a slide show from playing on the lock screen. The recommended state for this setting is: Enabled.

Rationale: Disabling the lock screen slide show extends the protection afforded by the lock screen to slide show contents.

CCE Reference Number: CCE-38348-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.1.1.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent Internet Explorer security prompt for Windows Installer scripts' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Installer\Prevent Internet Explorer security prompt for Windows Installer scripts>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting controls whether Web-based programs are allowed to install software on the computer without notifying the user. The recommended state for this setting is: Disabled.

Rationale: Suppressing the system warning can pose a security risk and increase the attack surface on the system.

CCE Reference Number: CCE-37524-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.74.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent the usage of OneDrive for file storage' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive\Prevent the usage of OneDrive for file storage

Note: This Group Policy path may not exist by default. An additional Group Policy template (SkyDrive.admx/adml) may be required - we strongly recommend you only use the version included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer). Older versions of the templates had conflicting settings in different template files for both OneDrive & SkyDrive, until it was cleaned up properly in the above version.

Impact: Users can't access OneDrive from the OneDrive app and file picker. Windows Store apps can't access OneDrive using the WinRT API. OneDrive doesn't appear in the navigation pane in File Explorer. OneDrive files aren't kept in sync with the cloud. Users can't automatically upload photos and videos from the camera roll folder.

Note: If your organization uses Office 365, be aware that this setting will prevent users from saving files to OneDrive/SkyDrive.

Vulnerability Details

This policy setting lets you prevent apps and features from working with files on OneDrive using the Next Generation Sync Client. The recommended state for this setting is: Enabled.

Rationale: Enabling this setting prevents users from accidentally uploading confidential or sensitive corporate information to the OneDrive cloud service using the Next Generation Sync Client.

CCE Reference Number: CCE-36939-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.47.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent the usage of SkyDrive for file storage' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting lets you prevent apps and features from working with files on SkyDrive. The recommended state for this setting is: Enabled.

Rationale: Enabling this setting prevents users from accidentally uploading confidential or sensitive corporate information to SkyDrive cloud service.

CCE Reference Number: CCE-33826-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.54.1

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\SkyDrive\Prevent the usage of SkyDrive for file storage

Note: This Group Policy path may not exist by default. An additional Group Policy template (SkyDrive.admx/adml) may be required - it is included with the Microsoft Windows 8.1/2012R2 Administrative Templates. Due to conflicting settings with the newer Windows 10 template of the same name, we recommend renaming the Windows 10 template to "OneDrive.admx/adml" before adding it to your ADMX repository or Central Store, so both versions can coexist. Likewise, ensure that any Windows 8.1/2012R2 versioned template is named "SkyDrive.admx/adml" before placing it in your ADMX repository or Central Store.

Impact: If you enable this policy setting: Users can't access SkyDrive from the SkyDrive app and file picker. Windows Store apps can't access SkyDrive using the WinRT API. SkyDrive doesn't appear in the navigation pane in File Explorer. SkyDrive files aren't kept in sync with the cloud. Users can't automatically upload photos and videos from the camera roll folder. If you disable or do not configure this policy setting apps and features can work with SkyDrive file storage.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent users from sharing files within their profile.' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\Prevent users from sharing files within their profile. Impact: If you enable this policy setting, users cannot share files within their profile using the sharing wizard. Also, the sharing wizard cannot create a share at %root%\users and can only be used to create SMB shares on folders.

Vulnerability Details

This policy setting specifies whether users can share files within their profile. By default users are allowed to share files within their profile to other users on their network after an administrator opts in the computer. An administrator can opt in the computer by using the sharing wizard to share a file within their profile. The recommended state for this setting is: Enabled.

Rationale: If not properly controlled a user could accidentally share sensitive data with unauthorized users. In a corporate environment, the company should provide a managed location for file sharing, such as a file server or SharePoint.

CCE Reference Number: CCE-38070-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 19.7.25.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prevent using Localhost IP address for WebRTC' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Prevent using Localhost IP address for WebRTC>

Impact: The employee's LocalHost IP address will be hidden while making phone calls using WebRTC.

Vulnerability Details

This setting lets you decide whether an employee's LocalHost IP address shows while making phone calls using the WebRTC protocol. The recommended state for this setting is: Enabled.

Rationale: WebRTC is a Real-Time Communications open source project supported by all major browsers. Allowing a system's local IP address to be shared may be considered a privacy concern.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.41.11

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Profile single process' is set to 'Administrators'

Trivial

Vulnerability Details

This policy setting determines which users can use tools to monitor the performance of non-system processes. Typically, you do not need to configure this user right to use the Microsoft Management Console (MMC) Performance snap-in. However, you do need this user right if System Monitor is configured to collect data using Windows Management Instrumentation (WMI). Restricting the Profile single process user right prevents intruders from gaining additional information that could be used to mount an attack on the system. The recommended state for this setting is: Administrators.

Rationale: The Profile single process user right presents a moderate vulnerability. An attacker with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. The attacker may also be able to determine what processes run on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software, an intrusion-detection system, or which other users are logged on to a computer.

CCE Reference Number: CCE-37131-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.34

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process Impact: If you remove the Profile single process user right from the Power Users group or other accounts, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks will not be negatively affected.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Profile single process' is set to 'Administrators' Trivial

Vulnerability Details

This policy setting determines which users can use tools to monitor the performance of non-system processes. Typically, you do not need to configure this user right to use the Microsoft Management Console (MMC) Performance snap-in. However, you do need this user right if System Monitor is configured to collect data using Windows Management Instrumentation (WMI). Restricting the Profile single process user right prevents intruders from gaining additional information that could be used to mount an attack on the system. The recommended state for this setting is: Administrators.

Rationale: The Profile single process user right presents a moderate vulnerability. An attacker with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. The attacker may also be able to determine what processes run on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software, an intrusion-detection system, or which other users are logged on to a computer.

CCE Reference Number: CCE-37131-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.34

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile single process>

Impact: If you remove the Profile single process user right from the Power Users group or other accounts, you could limit the abilities of users who are assigned to specific administrative roles in your environment. You should ensure that delegated tasks will not be negatively affected.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, NT SERVICE\WdiServiceHost : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance Impact: None. This is the default configuration.

Vulnerability Details

This policy setting allows users to use tools to view the performance of different system processes, which could be abused to allow attackers to determine a system's active processes and provide insight into the potential attack surface of the computer. The recommended state for this setting is: Administrators, NT SERVICE\WdiServiceHost.

Rationale: The Profile system performance user right poses a moderate vulnerability. Attackers with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. Attackers may also be able to determine what processes are active on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software or an intrusion detection system.

CCE Reference Number: CCE-36052-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.35

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Profile system performance' is set to 'Administrators, NT SERVICE\WdiServiceHost'

Trivial

Vulnerability Details

This policy setting allows users to use tools to view the performance of different system processes, which could be abused to allow attackers to determine a system's active processes and provide insight into the potential attack surface of the computer. The recommended state for this setting is: Administrators, NT SERVICE\WdiServiceHost.

Rationale: The Profile system performance user right poses a moderate vulnerability. Attackers with this user right could monitor a computer's performance to help identify critical processes that they might wish to attack directly. Attackers may also be able to determine what processes are active on the computer so that they could identify countermeasures that they may need to avoid, such as antivirus software or an intrusion detection system.

CCE Reference Number: CCE-36052-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.35

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators, NT SERVICE\WdiServiceHost:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Profile system performance>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Prohibit access of the Windows Connect Now wizards' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Network\Network\Windows Connect Now\Prohibit access of the Windows Connect Now wizards>

Impact: The WCN wizards are turned off and users have no access to any of the wizard tasks. All the configuration related tasks including "Set up a wireless router or access point" and "Add a wireless device" are disabled.

Vulnerability Details

This policy setting prohibits access to Windows Connect Now (WCN) wizards. The recommended state for this setting is: Enabled.

Rationale: Allowing standard users to access the Windows Connect Now wizard increases the risk and attack surface.

CCE Reference Number: CCE-36109-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.20.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prohibit connection to non-domain networks when connected to domain authenticated network' is set to 'Enabled' (MS only)

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Network\Windows Connection Manager\Prohibit connection to non-domain networks when connected to domain authenticated network>

Impact: The computer responds to automatic and manual network connection attempts based on the following circumstances: Automatic connection attempts - When the computer is already connected to a domain based network, all automatic connection attempts to non-domain networks are blocked. - When the computer is already connected to a non-domain based network, automatic connection attempts to domain based networks are blocked. Manual connection attempts - When the computer is already connected to either a non-domain based network or a domain based network over media other than Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing network connection is disconnected and the manual connection is allowed. - When the computer is already connected to either a non-domain based network or a domain based network over Ethernet, and a user attempts to create a manual connection to an additional network in violation of this policy setting, the existing Ethernet connection is maintained and the manual connection attempt is blocked.

Vulnerability Details

This policy setting prevents computers from connecting to both a domain based network and a non-domain based network at the same time. The recommended state for this setting is: Enabled.

Rationale: The potential concern is that a user would unknowingly allow network traffic to flow between the insecure public network and the managed corporate network.

CCE Reference Number: CCE-37627-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.21.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled : Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network Impact: The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A network bridge thus allows a computer that has connections to two different networks to share data between those networks. In an enterprise environment, where there is a need to control network traffic to only authorized paths, you can disable the Network Bridge setting on a computer. If you disable Network Bridge on a computer, users cannot create or configure a network bridge. Membership in the local Administrators group, or equivalent, is the minimum required to complete this procedure.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

You can use this procedure to enable or disable the user's ability to install and configure a network bridge. The recommended state for this setting is: Enabled.

Rationale: Allowing users to create a network bridge increases the risk and attack surface from the bridged network.

CCE Reference Number: CCE-38002-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.4.10.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prohibit installation and configuration of Network Bridge on your DNS domain network' is set to 'Enabled'

Trivial

Vulnerability Details

You can use this procedure to controls user's ability to install and configure a network bridge. The recommended state for this setting is: Enabled.

Rationale: The Network Bridge setting, if enabled, allows users to create a Layer 2 Media Access Control (MAC) bridge, enabling them to connect two or more physical network segments together. A network bridge thus allows a computer that has connections to two different networks to share data between those networks. In an enterprise environment, where there is a need to control network traffic to only authorized paths, allowing users to create a network bridge increases the risk and attack surface from the bridged network.

CCE Reference Number: CCE-38002-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.11.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Prohibit installation and configuration of Network Bridge on your DNS domain network>

Impact: Users cannot create or configure a network bridge.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Prohibit use of Internet Connection Sharing on your DNS domain network' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Prohibit use of Internet Connection Sharing on your DNS domain network>

Impact: Mobile Hotspot cannot be enabled or configured by Administrators and non-Administrators alike.

Vulnerability Details

Although this "legacy" setting traditionally applied to the use of Internet Connection Sharing (ICS) in Windows 2000, Windows XP & Server 2003, this setting now freshly applies to the Mobile Hotspot feature in Windows 10 & Server 2016. The recommended state for this setting is: Enabled.

Rationale: Non-administrators should not be able to turn on the Mobile Hotspot feature and open their Internet connectivity up to nearby mobile devices.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.11.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE : Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token Impact: On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

Vulnerability Details

This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE.

Note: A server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Rationale: User with the Replace a process level token privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000-based computers, use of the Replace a process level token user right also requires the user to have the Adjust memory quotas for a process user right that is discussed earlier in this section.)

CCE Reference Number: CCE-37430-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.36

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Replace a process level token' is set to 'LOCAL SERVICE, NETWORK SERVICE'

Trivial

Vulnerability Details

This policy setting allows one process or service to start another service or process with a different security access token, which can be used to modify the security access token of that sub-process and result in the escalation of privileges. The recommended state for this setting is: LOCAL SERVICE, NETWORK SERVICE.

Note: A Member Server that holds the Web Server (IIS) Role with Web Server Role Service will require a special exception to this recommendation, to allow IIS application pool(s) to be granted this user right.

Note #2: A Member Server with Microsoft SQL Server installed will require a special exception to this recommendation for additional SQL-generated entries to be granted this user right.

Rationale: User with the Replace a process level token privilege are able to start processes as other users whose credentials they know. They could use this method to hide their unauthorized actions on the computer. (On Windows 2000-based computers, use of the Replace a process level token user right also requires the user to have the Adjust memory quotas for a process user right that is discussed earlier in this section.)

CCE Reference Number: CCE-37430-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.36

Solution Details

To establish the recommended configuration via GP, set the following UI path to LOCAL SERVICE, NETWORK SERVICE:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Replace a process level token>

Impact: On most computers, this is the default configuration and there will be no negative impact. However, if you have installed the Web Server (IIS) Role with Web Services Role Service, you will need to allow the IIS application pool(s) to be granted this User Right Assignment.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Require a password when a computer wakes (on battery)' is set to 'Enabled' — Trivial

Vulnerability Details

Specifies whether or not the user is prompted for a password when the system resumes from sleep. The recommended state for this setting is: Enabled.

Rationale: Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

CCE Reference Number: CCE-36881-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.29.5.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (on battery)>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Require a password when a computer wakes (plugged in)' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Power Management\Sleep Settings\Require a password when a computer wakes (plugged in)>

Impact: None - this is the default configuration.

Vulnerability Details

Specifies whether or not the user is prompted for a password when the system resumes from sleep. The recommended state for this setting is: Enabled.

Rationale: Enabling this setting ensures that anyone who wakes an unattended computer from sleep state will have to provide logon credentials before they can access the system.

CCE Reference Number: CCE-37066-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.29.5.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	Trivial

Vulnerability Details

This policy setting determines whether to require domain users to elevate when setting a network's location. The recommended state for this setting is: Enabled.

Rationale: Allowing regular users to set a network location increases the risk and attack surface.

CCE Reference Number: CCE-38188-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.4.10.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Require domain users to elevate when setting a network's location Impact: If you enable this policy setting domain users must elevate when setting a network's location. If you disable or do not configure this policy setting domain users can set a network's location without elevating.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Require domain users to elevate when setting a network's location' is set to 'Enabled'	Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting determines whether to require domain users to elevate when setting a network's location. The recommended state for this setting is: Enabled.

Rationale: Allowing regular users to set a network location increases the risk and attack surface.

CCE Reference Number: CCE-38188-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.11.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Network\Network Connections\Require domain users to elevate when setting a network's location>

Impact: Domain users must elevate when setting a network's location.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Require pin for pairing' is set to 'Enabled' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Connect\Require pin for pairing

Note: This Group Policy path does not exist by default. An updated Group Policy template (WirelessDisplay.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: The pairing ceremony for connecting to new wireless display devices will always require a PIN.

Vulnerability Details

This policy setting controls whether or not a PIN is required for pairing to a wireless display device. The recommended state for this setting is: Enabled.

Rationale: If this setting is not configured or disabled then a PIN would not be required when pairing wireless display devices to the system, increasing the risk of unauthorized use.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.14.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication Impact: If you enable this policy setting, the terminal server accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

Vulnerability Details

This policy setting allows you to specify whether a terminal server requires secure remote procedure call (RPC) communication with all clients or allows unsecured communication. You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests. The recommended state for this setting is: Enabled.

Rationale: Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

CCE Reference Number: CCE-37567-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.48.3.9.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Require secure RPC communication' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting allows you to specify whether a terminal server requires secure remote procedure call (RPC) communication with all clients or allows unsecured communication. You can use this policy setting to strengthen the security of RPC communication with clients by allowing only authenticated and encrypted requests. The recommended state for this setting is: Enabled.

Rationale: Allowing unsecure RPC communication can exposes the server to man in the middle attacks and data disclosure attacks.

CCE Reference Number: CCE-37567-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.9.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Require secure RPC communication>

Impact: Remote Desktop Services accepts requests from RPC clients that support secure requests, and does not allow unsecured communication with untrusted clients.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' | Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 15 or more minute(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after Impact: If you do not configure this policy setting or if the value is configured to an interval that is too long, a DoS attack could occur. An attacker could maliciously attempt to log on to each user's account numerous times and lock out their accounts as described in the preceding paragraphs. If you do not configure the Reset account lockout counter after setting, administrators would have to manually unlock all accounts. If you configure this policy setting to a reasonable value the users would be locked out for some period, after which their accounts would unlock automatically. Be sure that you notify users of the values used for this policy setting so that they will wait for the lockout timer to expire before they call the help desk about their inability to log on.

Vulnerability Details

This policy setting determines the length of time before the Account lockout threshold resets to zero. The default value for this policy setting is Not Defined. If the Account lockout threshold is defined, this reset time must be less than or equal to the value for the Account lockout duration setting. If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts. If no policy were determined to reset the account lockout, it would be a manual task for administrators. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically. The recommended state for this setting is: 15 or more minute(s).

Rationale: Users can accidentally lock themselves out of their accounts if they mistype their password multiple times. To reduce the chance of such accidental lockouts, the Reset account lockout counter after setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers lockouts is reset to 0.

CCE Reference Number: CCE-36883-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 1.2.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Reset account lockout counter after' is set to '15 or more minute(s)' — Trivial

Vulnerability Details

This policy setting determines the length of time before the Account lockout threshold resets to zero. The default value for this policy setting is Not Defined. If the Account lockout threshold is defined, this reset time must be less than or equal to the value for the Account lockout duration setting. If you leave this policy setting at its default value or configure the value to an interval that is too long, your environment could be vulnerable to a DoS attack. An attacker could maliciously perform a number of failed logon attempts on all users in the organization, which will lock out their accounts. If no policy were determined to reset the account lockout, it would be a manual task for administrators. Conversely, if a reasonable time value is configured for this policy setting, users would be locked out for a set period until all of the accounts are unlocked automatically. The recommended state for this setting is: 15 or more minute(s).

Rationale: Users can accidentally lock themselves out of their accounts if they mistype their password multiple times. To reduce the chance of such accidental lockouts, the Reset account lockout counter after setting determines the number of minutes that must elapse before the counter that tracks failed logon attempts and triggers lockouts is reset to 0.

CCE Reference Number: CCE-36883-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 1.2.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to 15 or more minute(s):

<Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Account Lockout Policy\Reset account lockout counter after>

Impact: If you do not configure this policy setting or if the value is configured to an interval that is too long, a DoS attack could occur. An attacker could maliciously attempt to log on to each user's account numerous times and lock out their accounts as described in the preceding paragraphs. If you do not configure the Reset account lockout counter after setting, administrators would have to manually unlock all accounts. If you configure this policy setting to a reasonable value the users would be locked out for some period, after which their accounts would unlock automatically. Be sure that you notify users of the values used for this policy setting so that they will wait for the lockout timer to expire before they call the help desk about their inability to log on.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Restore files and directories' is set to 'Administrators'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories Impact: If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

Vulnerability Details

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right. The recommended state for this setting is: Administrators.

Rationale: An attacker with the Restore files and directories user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer.

Note: Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that are used to back up data.

CCE Reference Number: CCE-37613-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.37

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Restore files and directories' is set to 'Administrators'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Restore files and directories>

Impact: If you remove the Restore files and directories user right from the Backup Operators group and other accounts you could make it impossible for users who have been delegated specific tasks to perform those tasks. You should verify that this change won't negatively affect the ability of your organization's personnel to do their jobs.

Vulnerability Details

This policy setting determines which users can bypass file, directory, registry, and other persistent object permissions when restoring backed up files and directories on computers that run Windows Vista in your environment. This user right also determines which users can set valid security principals as object owners; it is similar to the Back up files and directories user right. The recommended state for this setting is: Administrators.

Rationale: An attacker with the Restore files and directories user right could restore sensitive data to a computer and overwrite data that is more recent, which could lead to loss of important data, data corruption, or a denial of service. Attackers could overwrite executable files that are used by legitimate administrators or system services with versions that include malicious software to grant themselves elevated privileges, compromise data, or install backdoors for continued access to the computer.

Note: Even if the following countermeasure is configured, an attacker could still restore data to a computer in a domain that is controlled by the attacker. Therefore, it is critical that organizations carefully protect the media that are used to back up data.

CCE Reference Number: CCE-37613-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.37

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Restrict Remote Desktop Services users to a single Remote Desktop Services session' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Connections\Restrict Remote Desktop Services users to a single Remote Desktop Services session>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows you to restrict users to a single Remote Desktop Services session. The recommended state for this setting is: Enabled.

Rationale: This setting ensures that users & administrators who Remote Desktop to a server will continue to use the same session - if they disconnect and reconnect, they will go back to the same session they were using before, preventing the creation of a second simultaneous session. This both prevents unnecessary resource usage by having the server host unnecessary additional sessions (which would put extra load on the server) and also ensures a consistency of experience for the user.

CCE Reference Number: CCE-37708-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Restrict Unauthenticated RPC clients' is set to 'Enabled: Authenticated' (MS only)

Trivial

Vulnerability Details

This policy setting controls how the RPC server runtime handles unauthenticated RPC clients connecting to RPC servers. This policy setting impacts all RPC applications. In a domain environment this policy setting should be used with caution as it can impact a wide range of functionality including group policy processing itself. Reverting a change to this policy setting can require manual intervention on each affected machine. This policy setting should never be applied to a domain controller. A client will be considered an authenticated client if it uses a named pipe to communicate with the server or if it uses RPC Security. RPC Interfaces that have specifically requested to be accessible by unauthenticated clients may be exempt from this restriction, depending on the selected value for this policy setting. -- "None" allows all RPC clients to connect to RPC Servers running on the machine on which the policy setting is applied. -- "Authenticated" allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy setting is applied. Exemptions are granted to interfaces that have requested them. -- "Authenticated without exceptions" allows only authenticated RPC Clients (per the definition above) to connect to RPC Servers running on the machine on which the policy setting is applied. No exceptions are allowed. This value has the potential to cause serious problems and is not recommended. Note: This policy setting will not be applied until the system is rebooted. The recommended state for this setting is: Enabled: Authenticated.

Rationale: Unauthenticated RPC communication can create a security vulnerability.

CCE Reference Number: CCE-36559-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.32.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Authenticated:

<Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call\Restrict Unauthenticated RPC clients>

Impact: Only authenticated RPC Clients will be allowed to connect to RPC servers running on the machine on which the policy setting is applied. Exemptions are granted to interfaces that have requested them.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Screen saver timeout' is set to 'Enabled: 900 seconds or fewer, but not 0'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 900 or fewer, but not 0: User Configuration\Policies\Administrative Templates\Control Panel\Personalization\Screen saver timeout Impact: The screen saver will automatically activate when the computer has been unattended for the amount of time specified. The impact should be minimal since the screen saver is enabled by default.

Vulnerability Details

If the Screen Saver Timeout setting is enabled, then the screen saver will be launched when the specified amount of time has passed since the last user action. Valid values range from 1 to 89,400 seconds (24 hours). The setting has no effect if the wait time is set to zero or no screen saver has been specified. The recommended state for this setting is: Enabled: 900 seconds or fewer, but not 0.

Rationale: If a user forgets to lock their computer when they walk away it is possible that a passerby will hijack it.

CCE Reference Number: CCE-37908-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 19.1.3.4

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Vulnerability Details

This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.The recommended state for this setting is: Disabled.

Note: Old events may or may not be retained according to the "Backup log automatically when full" policy setting.

Rationale: If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37145-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.24.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Security: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log

Service\Security\Control Event Log behavior when the log file reaches its maximum size>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting controls Event Log behavior when the log file reaches its maximum size. The recommended state for this setting is: Disabled.

Note: Old events may or may not be retained according to the "Backup log automatically when full" policy setting.

Rationale: If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37145-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.26.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 196,608 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed. The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data. Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Vulnerability Details

This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 196,608 or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37695-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.24.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Security: Specify the maximum log file size (KB)' is set to 'Enabled: 196,608 or greater'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 196,608 or greater:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Security\Specify the maximum log file size (KB)>

Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed. The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data. Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Vulnerability Details

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. The recommended state for this setting is: Enabled: 196,608 or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37695-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.26.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Select when Feature Updates are received' is set to 'Enabled: Current Branch for Business, 180 days' — Trivial

Vulnerability Details

This policy setting determines what type of feature updates to receive, and when. The branch readiness level for each new Windows 10 feature update is initially considered a "Current Branch" (CB) release, to be used by organizations for initial deployments. Once Microsoft has verified the feature update should be considered for enterprise deployment, it will be declared a branch readiness level of "Current Branch for Business" (CBB). The recommended state for this setting is: Enabled: Current Branch for Business, 180 days.

Note: If the "Allow Telemetry" policy is set to 0, this policy will have no effect.

Rationale: Forcing new features without prior testing in your environment could cause software incompatibilities as well as introducing new bugs into the operating system. In a controlled corporate environment, it is generally preferred to delay the feature updates until thorough testing and a deployment plan is in place. This recommendation delays the automatic installation of new features as long as possible. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.90.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Current Branch for Business, 180 days: Computer Configuration\Policies\Administrative Templates\Windows

Components\Windows Update\Defer Windows Updates\Select when Feature Updates are received

Note: This Group Policy path does not exist by default. An updated Group Policy template (WindowsUpdate.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: Feature Updates will be delayed until 180 days after they are declared to have a branch readiness level of "Current Branch for Business" (CBB).

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Select when Quality Updates are received' is set to 'Enabled: 0 days' — Trivial

Vulnerability Details

This settings controls when Quality Updates are received. The recommended state for this setting is: Enabled: 0 days.

Note: If the "Allow Telemetry" policy is set to 0, this policy will have no effect.

Rationale: Quality Updates can contain important bug fixes and/or security patches, and should be installed as soon as possible. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.90.1.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:0 days: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\Defer Windows Updates\Select when Quality Updates are received

Note: This Group Policy path does not exist by default. An updated Group Policy template (WindowsUpdate.admx/adml) is required - it is included with the Microsoft Windows 10 Release 1607 & Server 2016 Administrative Templates (or newer).

Impact: None - this is the default behavior.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

Trivial

Vulnerability Details

This policy setting specifies whether the computer that is about to host the remote connection will enforce an encryption level for all data sent between it and the client computer for the remote session. The recommended state for this setting is Enabled: High Level.

Rationale: If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic.

CCE Reference Number: CCE-36627-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.48.3.9.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: High Level: Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption level Impact: Clients that do not support 128-bit encryption will be unable to establish Terminal Server sessions.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Set client connection encryption level' is set to 'Enabled: High Level'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: High Level:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\Set client connection encryption level>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting specifies whether to require the use of a specific encryption level to secure communications between client computers and RD Session Host servers during Remote Desktop Protocol (RDP) connections. This policy only applies when you are using native RDP encryption. However, native RDP encryption (as opposed to SSL encryption) is not recommended. This policy does not apply to SSL encryption. The recommended state for this setting is: Enabled: High Level.

Rationale: If Terminal Server client connections are allowed that use low level encryption, it is more likely that an attacker will be able to decrypt any captured Terminal Services network traffic.

CCE Reference Number: CCE-36627-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.9.3

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Do not execute any autorun commands: Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun Impact: If you enable this policy setting, an Administrator can change the default Windows Vista or later behavior for autorun to: a) Completely disable autorun commands, or b) Revert back to pre-Windows Vista behavior of automatically executing the autorun command.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines. The recommended state for this setting is: Enabled: Do not execute any autorun commands.

Rationale: Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior starting with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

CCE Reference Number: CCE-38217-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.8.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Set the default behavior for AutoRun' is set to 'Enabled: Do not execute any autorun commands'

Trivial

Vulnerability Details

This policy setting sets the default behavior for Autorun commands. Autorun commands are generally stored in autorun.inf files. They often launch the installation program or other routines. The recommended state for this setting is: Enabled: Do not execute any autorun commands.

Rationale: Prior to Windows Vista, when media containing an autorun command is inserted, the system will automatically execute the program without user intervention. This creates a major security concern as code may be executed without user's knowledge. The default behavior starting with Windows Vista is to prompt the user whether autorun command is to be run. The autorun command is represented as a handler in the Autoplay dialog.

CCE Reference Number: CCE-38217-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.8.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Do not execute any autorun commands:

<Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Set the default behavior for AutoRun>

Impact: AutoRun commands will be completely disabled.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Set time limit for active but idle Remote Desktop Services sessions' is set to 'Enabled: 15 minutes or less'	Trivial

Vulnerability Details

This policy setting allows you to specify the maximum amount of time that an active Remote Desktop Services session can be idle (without user input) before it is automatically disconnected. The recommended state for this setting is: Enabled: 15 minutes or less.

Rationale: This setting helps to prevent active Remote Desktop sessions from tying up the computer for long periods of time while not in use, preventing computing resources from being consumed by large numbers of inactive sessions. In addition, old, forgotten Remote Desktops session that are still active can cause password lockouts if the user's password has changed but the old session is still running. For systems that limit the number of connected users (e.g. servers in the default Administrative mode - 2 sessions only), other users' old but still active sessions can prevent another user from connecting, resulting in an effective denial of service.

CCE Reference Number: CCE-37562-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.10.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 15 minutes or less:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set time limit for active but idle Remote Desktop Services sessions>

Impact: Remote Desktop Services will automatically disconnect active but idle sessions after 15 minutes (or the specified amount of time). The user receives a warning two minutes before the session disconnects, which allows the user to press a key or move the mouse to keep the session active. If you have a console session, idle session time limits do not apply.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Set time limit for disconnected sessions' is set to 'Enabled: 1 minute' | Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: 1 minute:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\Set time limit for disconnected sessions>

Impact: Disconnected Remote Desktop sessions are deleted from the server after 1 minute. If you have a console session, disconnected session time limits do not apply.

Vulnerability Details

This policy setting allows you to configure a time limit for disconnected Remote Desktop Services sessions. The recommended state for this setting is: Enabled: 1 minute.

Rationale: This setting helps to prevent active Remote Desktop sessions from tying up the computer for long periods of time while not in use, preventing computing resources from being consumed by large numbers of disconnected but still active sessions. In addition, old, forgotten Remote Desktops session that are still active can cause password lockouts if the user's password has changed but the old session is still running. For systems that limit the number of connected users (e.g. servers in the default Administrative mode - 2 sessions only), other users' old but still active sessions can prevent another user from connecting, resulting in an effective denial of service. This setting is important to ensure a disconnected session is properly terminated.

CCE Reference Number: CCE-37949-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.52.3.10.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' | Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log

Service\Setup\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Vulnerability Details

This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled.

Note: Old events may or may not be retained according to the "Backup log automatically when full" policy setting.

Rationale: If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-38276-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.24.3.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Setup: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Control Event Log behavior when the log file reaches its maximum size>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting controls Event Log behavior when the log file reaches its maximum size. The recommended state for this setting is: Disabled.

Note: Old events may or may not be retained according to the "Backup log automatically when full" policy setting.

Rationale: If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-38276-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.26.3.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed. The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data. Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Vulnerability Details

This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

CCE Reference Number: CCE-37526-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.24.3.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Setup: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\Specify the maximum log file size (KB)>

Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed. The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data. Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Vulnerability Details

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. The recommended state for this setting is: Enabled: 32,768 or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

CCE Reference Number: CCE-37526-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.26.3.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled'

Trivial

Vulnerability Details

This policy setting determines whether a computer can be shut down when a user is not logged on. If this policy setting is enabled, the shutdown command is available on the Windows logon screen. It is recommended to disable this policy setting to restrict the ability to shut down the computer to users with credentials on the system. The recommended state for this setting is: Disabled.

Rationale: Users who can access the console locally could shut down the computer.Attackers could also walk to the local console and restart the server, which would cause a temporary DoS condition. Attackers could also shut down the server and leave all of its applications and services unavailable.

CCE Reference Number: CCE-36788-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.13.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on Impact: Operators will have to log on to servers to shut them down or restart them.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Shutdown: Allow system to be shut down without having to log on' is set to 'Disabled'

Trivial

Vulnerability Details

This policy setting determines whether a computer can be shut down when a user is not logged on. If this policy setting is enabled, the shutdown command is available on the Windows logon screen. It is recommended to disable this policy setting to restrict the ability to shut down the computer to users with credentials on the system. The recommended state for this setting is: Disabled.

Note: In Server 2008 R2 and older versions, this setting had no impact on Remote Desktop (RDP) / Terminal Services sessions - it only affected the local console. However, Microsoft changed the behavior in Windows Server 2012 (non-R2) and above, where if set to Enabled, RDP sessions are also allowed to shut down or restart the server.

Rationale: Users who can access the console locally could shut down the computer. Attackers could also walk to the local console and restart the server, which would cause a temporary DoS condition. Attackers could also shut down the server and leave all of its applications and services unavailable. As noted in the Description above, the Denial of Service (DoS) risk of enabling this setting dramatically increases in Windows Server 2012 (non-R2) and above, as even remote users can shut down or restart the server.

CCE Reference Number: CCE-36788-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.13.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Shutdown: Allow system to be shut down without having to log on>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Shut down the system' is set to 'Administrators'

Trivial

Vulnerability Details

This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial of service condition. The recommended state for this setting is: Administrators.

Rationale: The ability to shut down domain controllers and member servers should be limited to a very small number of trusted administrators. Although the Shut down the system user right requires the ability to log on to the server, you should be very careful about which accounts and groups you allow to shut down a domain controller or member server. When a domain controller is shut down, it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down domain controllers that possess Flexible Single Master Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwords#x2014;the Primary Domain Controller (PDC) Emulator role.

CCE Reference Number: CCE-38328-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.38

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system Impact: The impact of removing these default groups from the Shut down the system user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Shut down the system' is set to 'Administrators' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Shut down the system>

Impact: The impact of removing these default groups from the Shut down the system user right could limit the delegated abilities of assigned roles in your environment. You should confirm that delegated activities will not be adversely affected.

Vulnerability Details

This policy setting determines which users who are logged on locally to the computers in your environment can shut down the operating system with the Shut Down command. Misuse of this user right can result in a denial of service condition. The recommended state for this setting is: Administrators.

Rationale: The ability to shut down domain controllers and member servers should be limited to a very small number of trusted administrators. Although the Shut down the system user right requires the ability to log on to the server, you should be very careful about which accounts and groups you allow to shut down a domain controller or member server. When a domain controller is shut down, it is no longer available to process logons, serve Group Policy, and answer Lightweight Directory Access Protocol (LDAP) queries. If you shut down domain controllers that possess Flexible Single Master Operations (FSMO) roles, you can disable key domain functionality, such as processing logons for new passwords the Primary Domain Controller (PDC) Emulator role.

CCE Reference Number: CCE-38328-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.38

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options\Sign-in last interactive user automatically after a system-initiated restart >

Impact: The user is required to present the logon credentials in order to proceed after restart.

Vulnerability Details

This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system. If you enable or do not configure this policy setting the device securely saves the user's credentials (including the user name domain and encrypted password) to configure automatic sign-in after a Windows Update restart. After the Windows Update restart the user is automatically signed-in and the session is automatically locked with all the lock screen apps configured for that user. If you disable this policy setting the device does not store the user's credentials for automatic sign-in after a Windows Update restart. The users' lock screen apps are not restarted after the system restarts. The recommended state for this setting is: Disabled.

Rationale: Disabling this feature will prevent the caching of user's credentials and unauthorized use of the device, and also ensure the user is aware of the restart.

CCE Reference Number: CCE-36977-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.70.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Sign-in last interactive user automatically after a system-initiated restart' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options\Sign-in last interactive user automatically after a system-initiated restart>

Impact: The device does not store the user's credentials for automatic sign-in after a Windows Update restart. The users' lock screen apps are not restarted after the system restarts. The user is required to present the logon credentials in order to proceed after restart.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting controls whether a device will automatically sign-in the last interactive user after Windows Update restarts the system. The recommended state for this setting is: Disabled.

Rationale: Disabling this feature will prevent the caching of user's credentials and unauthorized use of the device, and also ensure the user is aware of the restart.

CCE Reference Number: CCE-36977-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.75.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption, which provides support for application protocols that require knowledge of the user's password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plain text versions of the passwords. The recommended state for this setting is: Disabled.

Rationale: Enabling this policy setting allows the operating system to store passwords in a weaker format that is much more susceptible to compromise and weakens your system security.

CCE Reference Number: CCE-36286-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 1.1.6

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption Impact: If your organization uses either the CHAP authentication protocol through remote access or IAS services or Digest Authentication in IIS, you must configure this policy setting to Enabled. This setting is extremely dangerous to apply through Group Policy on a user-by-user basis, because it requires the appropriate user account object to be opened in Active Directory Users and Computers.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Store passwords using reversible encryption' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Store passwords using reversible encryption>

Impact: If your organization uses either the CHAP authentication protocol through remote access or IAS services or Digest Authentication in IIS, you must configure this policy setting to Enabled. This setting is extremely dangerous to apply through Group Policy on a user-by-user basis, because it requires the appropriate user account object to be opened in Active Directory Users and Computers.

Vulnerability Details

This policy setting determines whether the operating system stores passwords in a way that uses reversible encryption, which provides support for application protocols that require knowledge of the user's password for authentication purposes. Passwords that are stored with reversible encryption are essentially the same as plaintext versions of the passwords. The recommended state for this setting is: Disabled.

Rationale: Enabling this policy setting allows the operating system to store passwords in a weaker format that is much more susceptible to compromise and weakens your system security.

CCE Reference Number: CCE-36286-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 1.1.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Support device authentication using certificate' is set to 'Enabled: Automatic'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Automatic:

<Computer Configuration\Policies\Administrative Templates\System\Kerberos\Support device authentication using certificate>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows you to set support for Kerberos to attempt authentication using the certificate for the device to the domain. Support for device authentication using certificate will require connectivity to a DC in the device account domain which supports certificate authentication for computer accounts. The recommended state for this setting is: Enabled: Automatic.

Rationale: Having stronger device authentication with the use of certificates is strongly encouraged over standard username and password authentication. Having this set to Automatic will allow certificate based authentication to be used whenever possible.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.23.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Synchronize directory service data' is set to 'No One' (DC only) — Trivial

Vulnerability Details

This security setting determines which users and groups have the authority to synchronize all directory service data. The recommended state for this setting is: No One.

Rationale: The Synchronize directory service data user right affects domain controllers; only domain controllers should be able to synchronize directory service data. Domain controllers have this user right inherently, because the synchronization process runs in the context of the System account on domain controllers. Attackers who have this user right can view all information stored within the directory. They could then use some of that information to facilitate additional attacks or expose sensitive data, such as direct telephone numbers or physical addresses.

CCE Reference Number: CCE-36099-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.39

Solution Details

To establish the recommended configuration via GP, set the following UI path to No One:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Synchronize directory service data>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System ASLR' is set to 'Enabled: Application Opt-In'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-In: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System ASLR

Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Vulnerability Details

This setting determines how applications become enrolled in address space layout randomization (ASLR). The recommended state for this setting is: Enabled: Application Opt-In.

Rationale: ASLR reduces the predictability of process memory, which in-turn helps reduce the reliability of exploits targeting memory corruption vulnerabilities.

CCE Reference Number: CCE-38437-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.22.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Control Event Log behavior when the log file reaches its maximum size Impact: If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events.

Vulnerability Details

This policy setting controls Event Log behavior when the log file reaches its maximum size. If you enable this policy setting and a log file reaches its maximum size, new events are not written to the log and are lost. If you disable or do not configure this policy setting and a log file reaches its maximum size, new events overwrite old events. The recommended state for this setting is: Disabled.

Note: Old events may or may not be retained according to the "Backup log automatically when full" policy setting.

Rationale: If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36160-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.24.4.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System: Control Event Log behavior when the log file reaches its maximum size' is set to 'Disabled'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log

Service\System\Control Event Log behavior when the log file reaches its maximum size>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting controls Event Log behavior when the log file reaches its maximum size. The recommended state for this setting is: Disabled.

Note: Old events may or may not be retained according to the "Backup log automatically when full" policy setting.

Rationale: If new events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36160-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.26.4.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System DEP' is set to 'Enabled: Application Opt-Out'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System DEP

Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Vulnerability Details

This setting determines how applications become enrolled in data execution protection (DEP). The recommended state for this setting is: Enabled: Application Opt-Out.

Rationale: DEP marks pages of application memory as non-executable, which reduces a given exploit's ability to run attacker-controlled code.

CCE Reference Number: CCE-38438-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.22.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32' subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX (POSIX). Because Windows is case insensitive (but the POSIX subsystem will support case sensitivity), failure to enforce this policy setting makes it possible for a user of the POSIX subsystem to create a file with the same name as another file by using mixed case to label it. Such a situation can block access to these files by another user who uses typical Win32 tools, because only one of the files will be available. The recommended state for this setting is: Enabled.

Rationale: Because Windows is case-insensitive but the POSIX subsystem will support case sensitivity, failure to enable this policy setting would make it possible for a user of that subsystem to create a file with the same name as another file but with a different mix of upper and lower case letters. Such a situation could potentially confuse users when they try to access such files from normal Win32 tools because only one of the files will be available.

CCE Reference Number: CCE-37885-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.15.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Require case insensitivity for non-Windows subsystems Impact: All subsystems will be forced to observe case insensitivity. This configuration may confuse users who are familiar with any UNIX-based operating systems that is case-sensitive.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System objects: Require case insensitivity for non-Windows subsystems' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Require case insensitivity for non-Windows subsystems>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32 subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX (POSIX). Because Windows is case insensitive (but the POSIX subsystem will support case sensitivity), failure to enforce this policy setting makes it possible for a user of the POSIX subsystem to create a file with the same name as another file by using mixed case to label it. Such a situation can block access to these files by another user who uses typical Win32 tools, because only one of the files will be available. The recommended state for this setting is: Enabled.

Rationale: Because Windows is case-insensitive but the POSIX subsystem will support case sensitivity, failure to enable this policy setting would make it possible for a user of that subsystem to create a file with the same name as another file but with a different mix of upper and lower case letters. Such a situation could potentially confuse users when they try to access such files from normal Win32 tools because only one of the files will be available.

CCE Reference Number: CCE-37885-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.15.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' | Trivial

Vulnerability Details

This policy setting determines the strength of the default discretionary access control list (DACL) for objects. The setting helps secure objects that can be located and shared among processes and its default configuration strengthens the DACL, because it allows users who are not administrators to read shared objects but does not allow them to modify any that they did not create. The recommended state for this setting is: Enabled.

Rationale: This setting determines the strength of the default DACL for objects. Windows Server 2003 maintains a global list of shared computer resources so that objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and with what permissions. If you enable this setting, the default DACL is strengthened because non-administrator users are allowed to read shared objects but not modify shared objects that they did not create.

CCE Reference Number: CCE-37644-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.15.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links) Impact: None. This is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)' is set to 'Enabled' | Trivial

Vulnerability Details

This policy setting determines the strength of the default discretionary access control list (DACL) for objects. Active Directory maintains a global list of shared system resources, such as DOS device names, mutexes, and semaphores. In this way, objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and what permissions are granted. The recommended state for this setting is: Enabled.

Rationale: This setting determines the strength of the default DACL for objects. Windows maintains a global list of shared computer resources so that objects can be located and shared among processes. Each type of object is created with a default DACL that specifies who can access the objects and with what permissions.

CCE Reference Number: CCE-37644-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.15.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System SEHOP' is set to 'Enabled: Application Opt-Out' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Application Opt-Out: Computer Configuration\Policies\Administrative Templates\Windows Components\EMET\System SEHOP

Note: This Group Policy path does not exist by default. An additional Group Policy template (EMET.admx/adml) is required - it is included with Microsoft Enhanced Mitigation Experience Toolkit (EMET).

Vulnerability Details

This setting determines how applications become enrolled in structured exception handler overwrite protection (SEHOP). The recommended state for this setting is: Enabled: Application Opt-Out.

Rationale: When a software component suffers from a memory corruption vulnerability, an exploit may be able to overwrite memory that contains data structures that control how the software handles exceptions. By corrupting these structures in a controlled manner, an exploit may be able to execute arbitrary code. SEHOP verifies the integrity of those structures before they are used to handle exceptions, which reduces the reliability of exploits that leverage structured exception handler overwrites.

CCE Reference Number: CCE-38439-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.22.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater: Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB) Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed. The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data. Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Vulnerability Details

This policy setting specifies the maximum size of the log file in kilobytes. If you enable this policy setting, you can configure the maximum log file size to be between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. If you disable or do not configure this policy setting, the maximum size of the log file will be set to the locally configured value. This value can be changed by the local administrator using the Log Properties dialog and it defaults to 20 megabytes. The recommended state for this setting is: Enabled: 32,768 or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

CCE Reference Number: CCE-36092-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.24.4.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'System: Specify the maximum log file size (KB)' is set to 'Enabled: 32,768 or greater'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Enabled: 32,768 or greater:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\System\Specify the maximum log file size (KB)>

Impact: When event logs fill to capacity, they will stop recording information unless the retention method for each is set so that the computer will overwrite the oldest entries with the most recent ones. To mitigate the risk of loss of recent data, you can configure the retention method so that older events are overwritten as needed. The consequence of this configuration is that older events will be removed from the logs. Attackers can take advantage of such a configuration, because they can generate a large number of extraneous events to overwrite any evidence of their attack. These risks can be somewhat reduced if you automate the archival and backup of event log data. Ideally, all specifically monitored events should be sent to a server that uses Microsoft System Center Operations Manager (SCOM) or some other automated monitoring tool. Such a configuration is particularly important because an attacker who successfully compromises a server could clear the Security log. If all events are sent to a monitoring server, then you will be able to gather forensic information about the attacker's activities.

Vulnerability Details

This policy setting specifies the maximum size of the log file in kilobytes. The maximum log file size can be configured between 1 megabyte (1,024 kilobytes) and 2 terabytes (2,147,483,647 kilobytes) in kilobyte increments. The recommended state for this setting is: Enabled: 32,768 or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users

CCE Reference Number: CCE-36092-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.26.4.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects Impact: None. This is the default configuration.

Vulnerability Details

This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user. The recommended state for this setting is: Administrators.

Rationale: Any users with the Take ownership of files or other objects user right can take control of any object, regardless of the permissions on that object, and then make any changes they wish to that object. Such changes could result in exposure of data, corruption of data, or a DoS condition.

CCE Reference Number: CCE-38325-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.2.40

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Take ownership of files or other objects' is set to 'Administrators' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Administrators:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Take ownership of files or other objects>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting allows users to take ownership of files, folders, registry keys, processes, or threads. This user right bypasses any permissions that are in place to protect objects to give ownership to the specified user. The recommended state for this setting is: Administrators.

Rationale: Any users with the Take ownership of files or other objects user right can take control of any object, regardless of the permissions on that object, and then make any changes they wish to that object. Such changes could result in exposure of data, corruption of data, or a DoS condition.

CCE Reference Number: CCE-38325-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.2.40

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Toggle user control over Insider builds' is set to 'Disabled' — Trivial

Vulnerability Details

This policy setting determines whether users can access the Insider build controls in the Advanced Options for Windows Update. These controls are located under "Get Insider builds," and enable users to make their devices available for downloading and installing Windows preview software. The recommended state for this setting is: Disabled.

Note: This policy setting applies only to devices running Windows 10 Pro, Windows 10 Enterprise, or Server 2016.

Rationale: It can be dangerous in an Enterprise environment if experimental features are allowed because this can introduce bugs and security holes into systems allowing an attacker to gain access.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.16.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Data Collection and Preview Builds\Toggle user control over Insider builds

Note: This Group Policy path does not exist by default. An additional Group Policy template (allowbuildpreview.admx/adml) is required - it is included with the Microsoft Windows 10 Administrative Templates.

Impact: The item "Get Insider builds" will be unavailable.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off access to the Store' is set to 'Enabled' Trivial

Vulnerability Details

This policy setting specifies whether to use the Store service for finding an application to open a file with an unhandled file type or protocol association. When a user opens a file type or protocol that is not associated with any applications on the computer, the user is given the choice to select a local application or use the Store service to find an application. The recommended state for this setting is: Enabled.

Rationale: The Store service is a retail outlet built into Windows, primarily for consumer use. In an enterprise environment the IT department should be managing the installation of all applications to reduce the risk of the installation of vulnerable software.

CCE Reference Number: CCE-37904-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication

Management\Internet Communication settings\Turn off access to the Store>

Impact: The "Look for an app in the Store" item in the Open With dialog is removed.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	**Trivial**

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off app notifications on the lock screen Impact: If you enable this policy setting, no app notifications are displayed on the lock screen. If you disable or do not configure this policy setting, users can choose which apps display notifications on the lock screen.

Vulnerability Details

This policy setting allows you to prevent app notifications from appearing on the lock screen. If you enable this policy setting, no app notifications are displayed on the lock screen. If you disable or do not configure this policy setting, users can choose which apps display notifications on the lock screen. The recommended state for this setting is: Enabled.

Rationale: App notifications might display sensitive business or personal data.

CCE Reference Number: CCE-35893-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.24.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off app notifications on the lock screen' is set to 'Enabled'	**Trivial**

Vulnerability Details

This policy setting allows you to prevent app notifications from appearing on the lock screen. The recommended state for this setting is: Enabled.

Rationale: App notifications might display sensitive business or personal data.

CCE Reference Number: CCE-35893-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.25.5

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Logon\Turn off app notifications on the lock screen>

Impact: No app notifications are displayed on the lock screen.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Microsoft Edge\Turn off Automatic Download and Install of updates Impact: If you disable this setting, the automatic download and installation of app updates is turned on.

Vulnerability Details

This setting enables or disables the automatic download and installation of app updates. The recommended state for this setting is: Disabled.

Rationale: Keeping your system properly patched can help protect against 0 day vulnerabilities.

CCE Reference Number: CCE-38360-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.58.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Automatic Download and Install of updates' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off Automatic Download and Install of updates>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This setting enables or disables the automatic download and installation of Windows Store app updates. The recommended state for this setting is: Disabled.

Rationale: Keeping your system properly patched can help protect against 0 day vulnerabilities.

CCE Reference Number: CCE-38360-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.61.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: All drives:

Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Turn off Autoplay Impact: Users will have to manually launch setup or installation programs that are provided on removable media.

Vulnerability Details

Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. You can enable the Turn off Autoplay setting to disable the Autoplay feature. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.

Note: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives. The recommended state for this setting is: Enabled: All drives.

Rationale: An attacker could use this feature to launch a program to damage a client computer or data on the computer.

CCE Reference Number: CCE-36875-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.8.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Autoplay' is set to 'Enabled: All drives' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: All drives:

<Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\Turn off Autoplay>

Impact: Autoplay will be disabled - users will have to manually launch setup or installation programs that are provided on removable media.

Vulnerability Details

Autoplay starts to read from a drive as soon as you insert media in the drive, which causes the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage the computer or data on the computer. Autoplay is disabled by default on some removable drive types, such as floppy disk and network drives, but not on CD-ROM drives.

Note: You cannot use this policy setting to enable Autoplay on computer drives in which it is disabled by default, such as floppy disk and network drives. The recommended state for this setting is: Enabled: All drives.

Rationale: An attacker could use this feature to launch a program to damage a client computer or data on the computer.

CCE Reference Number: CCE-36875-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.8.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Group Policy\Turn off background refresh of Group Policy Impact: None - this is the default behavior. If you enable this policy setting the system waits until the current user logs off the system before updating the computer and user settings. If you disable or do not configure this policy setting updates can be applied while users are working. The frequency of updates is determined by the "Set Group Policy refresh interval for computers" and "Set Group Policy refresh interval for users" policy settings.

Note: If you make changes to this policy setting you must restart your computer for it to take effect.

Vulnerability Details

This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users and domain controllers. The recommended state for this setting is: Disabled.

Rationale: Setting this option to false (unchecked) will ensure that group policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

CCE Reference Number: CCE-37712-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.18.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off background refresh of Group Policy' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Administrative Templates\System\Group Policy\Turn off background refresh of Group Policy>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting prevents Group Policy from being updated while the computer is in use. This policy setting applies to Group Policy for computers, users and domain controllers. The recommended state for this setting is: Disabled.

Rationale: This setting ensures that group policy changes take effect more quickly, as compared to waiting until the next user logon or system restart.

CCE Reference Number: CCE-37712-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.19.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer Impact: Enabling this policy setting may allow certain legacy plug-in applications to function. Disabling this policy setting will ensure that Data Execution Prevention blocks certain types of malware from exploiting Explorer.

Vulnerability Details

Disabling data execution prevention can allow certain legacy plug-in applications to function without terminating Explorer. The recommended state for this setting is: Disabled.

Rationale: Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

CCE Reference Number: CCE-37809-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.28.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Data Execution Prevention for Explorer' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off Data Execution Prevention for Explorer>

Impact: None - this is the default configuration.

Vulnerability Details

Disabling data execution prevention can allow certain legacy plug-in applications to function without terminating Explorer. The recommended state for this setting is: Disabled.

Note: Some legacy plug-in applications and other software may not function with Data Execution Prevention and will require an exception to be defined for that specific plug-in/software.

Rationale: Data Execution Prevention is an important security feature supported by Explorer that helps to limit the impact of certain types of malware.

CCE Reference Number: CCE-37809-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.30.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off downloading of print drivers over HTTP' is set to 'Enabled'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off downloading of print drivers over HTTP>

Impact: Print drivers cannot be downloaded over HTTP.

Note: This policy setting does not prevent the client computer from printing to printers on the intranet or the Internet over HTTP. It only prohibits downloading drivers that are not already installed locally.

Vulnerability Details

This policy setting controls whether the computer can download print driver packages over HTTP. To set up HTTP printing, printer drivers that are not available in the standard operating system installation might need to be downloaded over HTTP. The recommended state for this setting is: Enabled.

Rationale: Users might download drivers that include malicious code.

CCE Reference Number: CCE-36625-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off handwriting personalization data sharing' is set to 'Enabled'

Trivial

Vulnerability Details

This setting turns off data sharing from the handwriting recognition personalization tool. The handwriting recognition personalization tool enables Tablet PC users to adapt handwriting recognition to their own writing style by providing writing samples. The tool can optionally share user writing samples with Microsoft to improve handwriting recognition in future versions of Windows. The tool generates reports and transmits them to Microsoft over a secure connection. The recommended state for this setting is: Enabled.

Rationale: A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many environments to automatically upload PII to a website without explicit approval by the user.

CCE Reference Number: CCE-37911-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriting personalization data sharing

Note: This Group Policy setting is provided by the Group Policy template "ShapeCollector.admx/adml" that is included with the Microsoft Windows 7/2008R2, 8/2012, 8.1/2012R2 and Windows 10 Administrative Templates. Impact: Tablet PC users cannot choose to share writing samples from the handwriting recognition personalization tool with Microsoft.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Turn off handwriting recognition error reporting' is set to 'Enabled'	Trivial

Vulnerability Details

Turns off the handwriting recognition error reporting tool. The handwriting recognition error reporting tool enables users to report errors encountered in Tablet PC Input Panel. The tool generates error reports and transmits them to Microsoft over a secure connection. Microsoft uses these error reports to improve handwriting recognition in future versions of Windows. The recommended state for this setting is: Enabled.

Rationale: A person's handwriting is Personally Identifiable Information (PII), especially when it comes to your signature. As such, it is unacceptable in many environments to automatically upload PII to a website without explicit approval by the user.

CCE Reference Number: CCE-36203-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off handwriting recognition error reporting>

Impact: Users cannot start the handwriting recognition error reporting tool or send error reports to Microsoft.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled'	Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Disabling this feature will prevent this. The recommended state for this setting is: Disabled.

Rationale: Allowing an application to function after its session has become corrupt increases the risk posture to the system.

CCE Reference Number: CCE-36660-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.28.4

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off heap termination on corruption Impact: Disabling heap termination on corruption can allow certain legacy plug-in applications to function without terminating Explorer immediately although Explorer may still terminate unexpectedly later.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off heap termination on corruption' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off heap termination on corruption>

Impact: None - this is the default configuration.

Vulnerability Details

Without heap termination on corruption, legacy plug-in applications may continue to function when a File Explorer session has become corrupt. Ensuring that heap termination on corruption is active will prevent this. The recommended state for this setting is: Disabled.

Rationale: Allowing an application to function after its session has become corrupt increases the risk posture to the system.

CCE Reference Number: CCE-36660-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.30.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com>

Impact: The "Choose a list of Internet Service Providers" path in the Internet Connection Wizard causes the wizard to exit. This prevents users from retrieving the list of ISPs, which resides on Microsoft servers.

Vulnerability Details

This policy setting specifies whether the Internet Connection Wizard can connect to Microsoft to download a list of Internet Service Providers (ISPs). The recommended state for this setting is: Enabled.

Rationale: In an Enterprise environment we want to lower the risk of a user unknowingly exposing sensitive data.

CCE Reference Number: CCE-37163-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Turn off Internet download for Web publishing and online ordering wizards' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting controls whether Windows will download a list of providers for the Web publishing and online ordering wizards. The recommended state for this setting is: Enabled.

Rationale: Although the risk is minimal, enabling this setting will reduce the possibility of a user unknowingly downloading malicious content through this feature.

CCE Reference Number: CCE-36096-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Internet download for Web publishing and online ordering wizards>

Impact: Windows is prevented from downloading providers; only the service providers cached in the local registry are displayed.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Turn off KMS Client Online AVS Validation' is set to 'Enabled'

Trivial

Vulnerability Details

The Key Management Service (KMS) is a Microsoft license activation method that entails setting up a local server that stores the licenses. The server itself needs to connect to Microsoft to activate the KMS service, but subsequent on-network clients can activate Microsoft Windows OS and/or their Microsoft

Office via the KMS server instead of connecting directly to Microsoft. This policy setting lets you opt-out of sending KMS client activation data to Microsoft automatically. The recommended state for this setting is: Enabled.

Rationale: Even though the KMS licensing method does not require a connection to Microsoft, the clients using KMS licensing still send KMS client activation state data to Microsoft automatically. Preventing this information from being sent can help reduce privacy concerns.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.59.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Software Protection Platform\Turn off KMS Client Online AVS Validation

Note: This Group Policy setting is provided by the Group Policy template "avsvalidationgp.admx/adml" that is included with the Microsoft Windows 10 Administrative Templates.

Impact: The computer is prevented from sending data to Microsoft regarding its KMS client activation state.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off location' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors\Turn off location>

Impact: The location feature is turned off, and all programs on this computer are prevented from using location information from the location feature.

Vulnerability Details

This policy setting turns off the location feature for the computer. The recommended state for this setting is: Enabled.

Rationale: This setting affects the location feature (e.g. GPS or other location tracking). From a security perspective, it's not a good idea to reveal your location to software in most cases, but there are legitimate uses, such as mapping software.

CCE Reference Number: CCE-36886-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.37.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Microsoft consumer experiences' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Turn off Microsoft consumer experiences>

Impact: Users will no longer see personalized recommendations from Microsoft and notifications about their Microsoft account.

Vulnerability Details

This policy setting turns off experiences that help consumers make the most of their devices and Microsoft account. The recommended state for this setting is: Enabled.

Note: Per Microsoft TechNet, this policy setting only applies to Windows 10 Enterprise and Windows 10 Education.

Rationale: Having apps silently installed in an environment is not good security practice - especially if the apps send data back to a 3rd party. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.13.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Turn off Microsoft Peer-to-Peer Networking Services' is set to 'Enabled'

Trivial

Vulnerability Details

The Peer Name Resolution Protocol (PNRP) allows for distributed resolution of a name to an IPV6 address and port number. The protocol operates in the context of clouds. A cloud is a set of peer computers that can communicate with each other by using the same IPv6 scope. Peer-to-Peer protocols allow for applications in the areas of RTC, collaboration, content distribution and distributed processing. The recommended state for this setting is: Enabled.

Rationale: This setting enhances the security of the environment and reduces the overall risk exposure related to peer-to-peer networking.

CCE Reference Number: CCE-37699-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.10.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services\Turn off Microsoft Peer-to-Peer Networking Services>

Impact: Microsoft Peer-to-Peer Networking Services are turned off in their entirety, and all applications dependent on them will stop working.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Turn off multicast name resolution' is set to 'Enabled' (MS Only)

Trivial

Vulnerability Details

LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client computer to another client computer on the same subnet that also has LLMNR enabled. LLMNR does not require a DNS server or DNS client configuration, and provides name resolution in scenarios in which conventional DNS name resolution is not possible. The recommended state for this setting is: Enabled.

Rationale: An attacker can listen on a network for these LLMNR (UDP/5355) or NBT-NS (UDP/137) broadcasts and respond to them, It can trick the host into thinking that it knows the location of the requested system.

Note: To completely mitigate local name resolution poisoning, in addition to this setting, the properties of each installed NIC should also be set to Disable NetBIOS over TCP/IP (on the WINS tab in the NIC properties). Unfortunately, there is no global setting to achieve this that automatically applies to all NICs - it is a per NIC setting that varies with different NIC hardware installations.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.4.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Network\DNS Client\Turn off multicast name resolution>

Impact: In the event DNS is unavailable a system will be unable to request it from other systems on the same subnet.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off printing over HTTP' is set to 'Enabled' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off printing over HTTP>

Impact: The client computer will not be able to print to Internet printers over HTTP.

Note: This policy setting affects the client side of Internet printing only. Regardless of how it is configured, a computer could act as an Internet Printing server and make its shared printers available through HTTP.

Vulnerability Details

This policy setting allows you to disable the client computer's ability to print over HTTP, which allows the computer to print to printers on the intranet as well as the Internet. The recommended state for this setting is: Enabled.

Rationale: Information that is transmitted over HTTP through this capability is not protected and can be intercepted by malicious users. For this reason, it is not often used in enterprise environments.

CCE Reference Number: CCE-36920-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Registration if URL connection is referring to Microsoft.com' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Registration if URL connection is referring to Microsoft.com>

Impact: Users are blocked from connecting to Microsoft.com for online registration and they cannot register their copy of Windows online.

Vulnerability Details

This policy setting specifies whether the Windows Registration Wizard connects to Microsoft.com for online registration. The recommended state for this setting is: Enabled.

Rationale: Users in a corporate environment should not be registering their own copies of Windows, providing their own PII in the process.

CCE Reference Number: CCE-36352-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Search Companion content file updates' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Search Companion content file updates>

Impact: Search Companion does not download content updates during searches.

Note: Internet searches will still send the search text and information about the search to Microsoft and the chosen search provider. If you select Classic Search, the Search Companion feature will be unavailable. You can select Classic Search by clicking Start, Search, Change Preferences, and then Change Internet Search Behavior.

Vulnerability Details

This policy setting specifies whether Search Companion should automatically download content updates during local and Internet searches. The recommended state for this setting is: Enabled.

Rationale: There is a small risk that users will unknowingly reveal sensitive information because of the topics they are searching for. This risk is very low because even if this setting is enabled users still must submit search queries to the desired search engine in order to perform searches.

CCE Reference Number: CCE-36884-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off shell protocol protected mode Impact: If you enable this policy setting the protocol is fully enabled allowing the opening of folders and files. If you disable this policy setting the protocol is in the protected mode allowing applications to only open a limited set of folders.

Vulnerability Details

This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows. The recommended state for this setting is: Disabled.

Rationale: Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

CCE Reference Number: CCE-36809-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.28.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off shell protocol protected mode' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\Turn off shell protocol protected mode>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows you to configure the amount of functionality that the shell protocol can have. When using the full functionality of this protocol applications can open folders and launch files. The protected mode reduces the functionality of this protocol allowing applications to only open a limited set of folders. Applications are not able to open files with this protocol when it is in the protected mode. It is recommended to leave this protocol in the protected mode to increase the security of Windows. The recommended state for this setting is: Disabled.

Rationale: Limiting the opening of files and folders to a limited set reduces the attack surface of the system.

CCE Reference Number: CCE-36809-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.30.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off the advertising ID' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\User Profiles\Turn off the advertising ID>

Impact: The advertising ID is turned off. Apps can't use the ID for experiences across apps.

Vulnerability Details

This policy setting turns off the advertising ID, preventing apps from using the ID for experiences across apps. The recommended state for this setting is: Enabled.

Rationale: Tracking user activity for advertising purposes, even anonymously, may be a privacy concern. In an enterprise environment, applications should not need or require tracking for targeted advertising.

CCE Reference Number: CCE-36931-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.41.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off the offer to update to the latest version of Windows Impact: If you enable this setting, the Store application will not offer updates to the latest version of Windows.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Enables or disables the Store offer to update to the latest version of Windows. The recommended state for this setting is: Enabled.

Rationale: Unplanned OS upgrades can lead to more preventable support calls. IT should be pushing only approved updates to the machine.

CCE Reference Number: CCE-38362-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.58.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off the offer to update to the latest version of Windows' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off the offer to update to the latest version of Windows>

Impact: The Windows Store application will not offer updates to the latest version of Windows.

Vulnerability Details

Enables or disables the Windows Store offer to update to the latest version of Windows. The recommended state for this setting is: Enabled.

Rationale: Unplanned OS upgrades can lead to more preventable support calls. The IT department should be managing and approving all updates.

CCE Reference Number: CCE-38362-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.61.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off the "Order Prints" picture task' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Order Prints" picture task>

Impact: The task "Order Prints Online" is removed from Picture Tasks in File Explorer folders.

Vulnerability Details

This policy setting specifies whether the "Order Prints Online" task is available from Picture Tasks in

Windows folders. The Order Prints Online Wizard is used to download a list of providers and allow users to order prints online. The recommended state for this setting is: Enabled.

Rationale: In an Enterprise environment we want to lower the risk of a user unknowingly exposing sensitive data.

CCE Reference Number: CCE-38275-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off the "Publish to Web" task for files and folders' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the "Publish to Web" task for files and folders>

Impact: The "Publish to Web" task is removed from File and Folder tasks in Windows folders.

Vulnerability Details

This policy setting specifies whether the tasks Publish this file to the Web, Publish this folder to the Web, and Publish the selected items to the Web are available from File and Folder Tasks in Windows folders. The recommended state for this setting is: Enabled.

Rationale: Users may publish confidential or sensitive information to a public service outside of the control of the organization.

CCE Reference Number: CCE-37090-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.11

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off the Store application' is set to 'Enabled' Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Store\Turn off the Store application>

Impact: Access to the Windows Store application is denied.

Vulnerability Details

This setting denies or allows access to the Store application. The recommended state for this setting is: Enabled.

Rationale: Only applications approved by an IT department should be installed. Allowing users to install 3rd party applications can lead to missed patches and potential zero day vulnerabilities.

CCE Reference Number: CCE-38363-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.61.4

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off the Windows Messenger Customer Experience Improvement Program' is set to 'Enabled' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off the Windows Messenger Customer Experience

Improvement Program>

Impact: Windows Messenger will not collect usage information, and the user settings to enable the collection of usage information will not be shown.

Vulnerability Details

This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used. Microsoft uses information collected through the Customer Experience Improvement Program to detect software flaws so that they can be corrected more quickly, enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose. The recommended state for this setting is: Enabled.

Rationale: Large enterprise environments may not want to have information collected from managed client computers.

CCE Reference Number: CCE-36628-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.12

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off toast notifications on the lock screen' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications\Turn off toast notifications on the lock screen Impact: By turning off this feature, applications will not be able to raise toast notifications on the lock screen, and user will not be able to access the information.

Vulnerability Details

This policy setting turns off toast notifications on the lock screen. If you enable this policy setting, applications will not be able to raise toast notifications on the lock screen. If you disable or do not configure this policy setting, toast notifications on the lock screen are enabled and can be turned off by the administrator or user. No reboots or service restarts are required for this policy setting to take effect. The recommended state for this setting is Enabled.

Rationale: While this feature can be handy for users applications that provide toast notifications might display sensitive personal or business data while the device is unattended.

CCE Reference Number: CCE-36332-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 19.5.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn off Windows Customer Experience Improvement Program' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Customer Experience Improvement Program>

Impact: All users are opted out of the Windows Customer Experience Improvement Program.

Vulnerability Details

This policy setting specifies whether Windows Messenger can collect anonymous information about how the Windows Messenger software and service is used. Microsoft uses information collected through the Windows Customer Experience Improvement Program to detect software flaws so that they can be corrected more quickly, enabling this setting will reduce the amount of data Microsoft is able to gather for this purpose. The recommended state for this setting is: Enabled.

Rationale: Large enterprise environments may not want to have information collected from managed client computers.

CCE Reference Number: CCE-36174-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.13

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Turn off Windows Error Reporting' is set to 'Enabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings\Turn off Windows Error Reporting>

Impact: Users are not given the option to report errors to Microsoft.

Vulnerability Details

This policy setting controls whether or not errors are reported to Microsoft. Error Reporting is used to report information about a system or application that has failed or has stopped responding and is used to improve the quality of the product. The recommended state for this setting is: Enabled.

Rationale: If a Windows Error occurs in a secure, managed corporate environment, the error should be reported directly to IT staff for troubleshooting and remediation. There is no benefit to the corporation to report these errors directly to Microsoft, and there is some risk of unknowingly exposing sensitive data as part of the error.

CCE Reference Number: CCE-35964-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.20.1.14

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'	Trivial

Vulnerability Details

This policy setting allows you to control whether a domain user can sign in using a convenience PIN. In Windows 10, convenience PIN was replaced with Passport, which has stronger security properties. To configure Passport for domain users, use the policies under Computer configuration\Administrative Templates\Windows Components\Microsoft Passport for Work. If you enable this policy setting, a domain user can set up and sign in with a convenience PIN. If you disable or don't configure this policy setting, a domain user can't set up and use a convenience PIN.

Note that the user's domain password will be cached in the system vault when using this feature. The recommended state for this setting is: Disabled.

Rationale: A PIN is created from a much smaller selection of characters than a password, so in most cases a PIN will be much less robust than a password.

CCE Reference Number: CCE-37528-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.8.24.5

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Logon\Turn on convenience PIN sign-in Note: In older Microsoft Windows Administrative Templates, this setting was simply named "Turn on PIN sign-in", but it was renamed as of the Windows 10 R1511 Administrative Templates. Impact: None - this is the default behavior.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn on convenience PIN sign-in' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\System\Logon\Turn on convenience PIN sign-in

Note: In older Microsoft Windows Administrative Templates, this setting was simply named "Turn on PIN sign-in", but it was renamed as of the Windows 10 Release 1511 Administrative Templates. Impact: None - this is the default configuration.

Vulnerability Details

This policy setting allows you to control whether a domain user can sign in using a convenience PIN. In Windows 10, convenience PIN was replaced with Passport, which has stronger security properties. To configure Passport for domain users, use the policies under Computer configuration\Administrative

Templates\Windows Components\Microsoft Passport for Work.

Note: The user's domain password will be cached in the system vault when using this feature. The recommended state for this setting is: Disabled.

Rationale: A PIN is created from a much smaller selection of characters than a password, so in most cases a PIN will be much less robust than a password.

CCE Reference Number: CCE-37528-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.25.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn on Mapper I/O (LLTDIO) driver' is set to 'Disabled'

Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled:

<Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Mapper I/O (LLTDIO) driver>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting changes the operational behavior of the Mapper I/O network protocol driver. LLTDIO allows a computer to discover the topology of a network it's connected to. It also allows a computer to initiate Quality-of-Service requests such as bandwidth estimation and network health analysis. The recommended state for this setting is: Disabled.

Rationale: To help protect from potentially discovering and connecting to unauthorized devices, We are recommending that this setting be disabled to guarantee the prevention of responding to network traffic for network topology discovery.

CCE Reference Number: CCE-38170-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.9.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Script Block Logging

Note: This Group Policy path does not exist by default. A newer version of the "powershellexecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates.

Impact: If you disable this policy setting, logging of PowerShell script input is disabled.

Vulnerability Details

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. The recommended state for this setting is: Disabled.

Rationale: Due to the potential risks of capturing passwords in the logs. This setting should only be needed for debugging purposes, and not in normal operation, it is important to ensure this is set to Disabled. CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.79.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn on PowerShell Script Block Logging' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Script Block Logging

Note: This Group Policy path does not exist by default. A newer version of the "powershellexecutionpolicy.admx/adml" Administrative Template is required - it is included with the Microsoft Windows 10 Administrative Templates.

Impact: Logging of PowerShell script input is disabled.

Vulnerability Details

This policy setting enables logging of all PowerShell script input to the Microsoft-Windows-PowerShell/Operational event log. The recommended state for this setting is: Disabled.

Note: In Microsoft's own hardening guidance, they recommend the opposite value, Enabled, because having this data logged improves investigations of PowerShell attack incidents. However, the default ACL on the PowerShell Operational log allows Interactive User (i.e. any logged on user) to read it, and therefore possibly expose passwords or other sensitive information to unauthorized users. If Microsoft locks down the default ACL on that log in the future (e.g. to restrict it only to Administrators), then we will revisit this recommendation in a future release.

Rationale: There are potential risks of capturing passwords in the PowerShell logs. This setting should only be needed for debugging purposes, and not in normal operation, it is important to ensure this is set to Disabled. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.84.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled : Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Transcription

Note: This Group Policy path does not exist by default. A newer version of the "powershellexecutionpolicy.admx/adml" Administrative Template is required - it is included with the

Microsoft Windows 10 Administrative Templates. Impact: If you disable this policy setting, transcription of PowerShell-based applications is disabled by default, although transcription can still be enabled through the Start-Transcript cmdlet.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts. The recommended state for this setting is: Disabled.

Rationale: If this setting is enabled there is a risk that passwords could get stored in plain text in the PowerShell_transcript output file.

CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.9.79.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn on PowerShell Transcription' is set to 'Disabled'	Trivial

Vulnerability Details

This Policy setting lets you capture the input and output of Windows PowerShell commands into text-based transcripts. The recommended state for this setting is: Disabled.

Rationale: If this setting is enabled there is a risk that passwords could get stored in plain text in the PowerShell_transcript output file. CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.84.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following Group Policy setting to Disabled: Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\Turn on PowerShell Transcription

Note: This Group Policy path does not exist by default. A newer version of the "powershellexecutionpolicy.admx/adml" Administrative Template is required - it is included with the

Microsoft Windows 10 Administrative Templates.

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Turn on Responder (RSPNDR) driver' is set to 'Disabled'	Trivial

Solution Details

To implement the recommended configuration state, set the following Group Policy setting to Disabled:

<Computer Configuration\Policies\Administrative Templates\Network\Link-Layer Topology Discovery\Turn on Responder (RSPNDR) driver>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting changes the operational behavior of the Responder network protocol driver. The Responder allows a computer to participate in Link Layer Topology Discovery requests so that it can be discovered and located on the network. It also allows a computer to participate in Quality-of-Service activities such as bandwidth estimation and network health analysis. The recommended state for this setting is: Disabled.

Rationale: To help protect from potentially discovering and connecting to unauthorized devices, We are recommending that this setting be disabled to guarantee the prevention of responding to network traffic for network topology discovery.

CCE Reference Number: CCE-37959-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.9.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Untrusted Font Blocking' is set to 'Enabled: Block untrusted fonts and log events'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Block untrusted fonts and log events:

<Computer Configuration\Policies\Administrative Templates\System\Mitigation Options\Untrusted Font Blocking>

Impact: Fonts not located in the %windir%\Fonts directory will not be loaded. This setting can temporarily be run in Audit mode ("Log events without blocking untrusted fonts") first to observe if blocking untrusted fonts would cause any usability or compatibility issues.

Vulnerability Details

This security feature provides a global setting to prevent programs from loading untrusted fonts. Untrusted fonts are any font installed outside of the %windir%\Fonts directory. This feature can be configured to be in 3 modes: On, Off, and Audit. The recommended state for this setting is: Enabled: Block untrusted fonts and log events

Rationale: Blocking untrusted fonts helps prevent both remote (web-based or email-based) and local EOP attacks that can happen during the font file-parsing process.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.8.26.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Use enhanced anti-spoofing when available' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting determines whether enhanced anti-spoofing is configured for devices which support it. The recommended state for this setting is: Enabled.

Rationale: Enterprise environments are now supporting a wider range of mobile devices, increasing the security on these devices will help protect against unauthorized access on your network.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.9.10.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Administrative Templates\Windows Components\Biometrics\Facial Features\Use enhanced anti-spoofing when available>

Impact: Windows will require all users on the device to use anti-spoofing for facial features, on devices which support it.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account Impact: Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege.

Vulnerability Details

This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account. The options are:- Enabled: The built-in Administrator account uses Admin Approval Mode. By default, any operation that requires elevation of privilege will prompt the user to approve the operation.- Disabled: (Default) The built-in Administrator account runs all applications with full administrative privilege. The recommended state for this setting is: Enabled.

Rationale: One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista the built-in Administrator account is disabled. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways:- If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator.- If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted. Once Windows Vista is installed, the built-in Administrator account may be enabled, but we strongly recommend that this account remain disabled.

CCE Reference Number: CCE-36494-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.17.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Admin Approval Mode for the Built-in Administrator account' is set to 'Enabled' — Trivial

Vulnerability Details

This policy setting controls the behavior of Admin Approval Mode for the built-in Administrator account. The recommended state for this setting is: Enabled.

Rationale: One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. An attack vector for these programs was to discover the password of the account named "Administrator" because that user account was created for all installations of Windows. To address this risk, in Windows Vista and newer, the built-in Administrator account is now disabled by default. In a default installation of a new computer, accounts with administrative control over the computer are initially set up in one of two ways: - If the computer is not joined to a domain, the first user account you create has the equivalent permissions as a local administrator. - If the computer is joined to a domain, no local administrator accounts are created. The Enterprise or Domain Administrator must log on to the computer and create one if a local administrator account is warranted. Once Windows is installed, the built-in Administrator account may be manually enabled, but we strongly recommend that this account remain disabled.

CCE Reference Number: CCE-36494-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.17.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Admin Approval Mode for the Built-in Administrator account>

Impact: The built-in Administrator account uses Admin Approval Mode. Users that log on using the local Administrator account will be prompted for consent whenever a program requests an elevation in privilege, just like any other user would.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop Impact: If you enable this setting, ("User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop), requests for elevation are automatically sent to the interactive desktop (not the secure desktop) and also appear on the remote administrator's view of the desktop during a Windows Remote Assistance session, and the remote administrator is able to provide the appropriate credentials for elevation. This setting does not change the behavior of the UAC elevation prompt for administrators.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This policy setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts used by a standard user.- Enabled: UIA programs, including Windows Remote Assistance, automatically disable the secure desktop for elevation prompts. If you do not disable the "User Account Control: Switch to the secure desktop when prompting for elevation" policy setting, the prompts appear on the interactive user's desktop instead of the secure desktop.- Disabled: (Default) The secure desktop can be disabled only by the user of the interactive desktop or by disabling the "User Account Control: Switch to the secure desktop when prompting for elevation" policy setting. The recommended state for this setting is: Disabled.

Rationale: One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting allows the administrator to perform operations that require elevated privileges while connected via Remote Assistance. This increases security in that organizations can use UAC even when end user support is provided remotely. However, it also reduces security by adding the risk that an administrator might allow an unprivileged user to share elevated privileges for an application that the administrator needs to use during the Remote Desktop session.

CCE Reference Number: CCE-36863-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.17.2

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop' is set to 'Disabled'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting controls whether User Interface Accessibility (UIAccess or UIA) programs can automatically disable the secure desktop for elevation prompts used by a standard user. The recommended state for this setting is: Disabled.

Rationale: One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting allows the administrator to perform operations that require elevated privileges while connected via Remote Assistance. This increases security in that organizations can use UAC even when end user support is provided remotely. However, it also reduces security by adding the risk that an administrator might allow an unprivileged user to share elevated privileges for an application that the administrator needs to use during the Remote Desktop session.

CCE Reference Number: CCE-36863-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.17.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Prompt for consent on the secure desktop: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode Impact: This policy setting controls the behavior of the elevation prompt for administrators.

Vulnerability Details

This policy setting controls the behavior of the elevation prompt for administrators. The options are:- Elevate without prompting: Allows privileged accounts to perform an operation that requires elevation without requiring consent or credentials. Note: Use this option only in the most constrained environments.- Prompt for credentials on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a privileged user name and password. If the user enters valid credentials, the operation continues with the user's highest available privilege.- Prompt for consent on the secure desktop: When an operation requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.- Prompt for consent: When an operation requires elevation of privilege, the user is prompted to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.- Prompt for consent for non-Windows binaries: (Default) When an operation for a non-Microsoft application requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege. The recommended state for this setting is: Prompt for consent on the secure desktop .

Rationale: One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

CCE Reference Number: CCE-37029-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.17.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode' is set to 'Prompt for consent on the secure desktop'

Trivial

Vulnerability Details

This policy setting controls the behavior of the elevation prompt for administrators. The recommended state for this setting is: Prompt for consent on the secure desktop.

Rationale: One of the risks that the UAC feature introduced with Windows Vista is trying to mitigate is that of malicious software running under elevated credentials without the user or administrator being aware of its activity. This setting raises awareness to the administrator of elevated privilege operations and permits the administrator to prevent a malicious program from elevating its privilege when the program attempts to do so.

CCE Reference Number: CCE-37029-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.17.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Prompt for consent on the secure desktop:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode>

Impact: When an operation (including execution of a Windows binary) requires elevation of privilege, the user is prompted on the secure desktop to select either Permit or Deny. If the user selects Permit, the operation continues with the user's highest available privilege.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Automatically deny elevation requests: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users Impact: Users will need to provide administrative passwords to be able to run programs with elevated privileges. This could cause an increased load on IT staff while the programs that are impacted are identified and standard operating procedures are modified to support least privilege operations.

Vulnerability Details

This policy setting controls the behavior of the elevation prompt for standard users. The options are: Prompt for credentials: When an operation requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. Automatically deny elevation requests: When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls. Prompt for credentials on the secure desktop: (Default) When an operation requires elevation of privilege, the user is prompted on the secure desktop to enter a different user name and password. If the user enters valid credentials, the operation continues with the applicable privilege. Note that this option was introduced in Windows 7 and it is not applicable to computers running Windows Vista or Windows Server 2008. The recommended state for this setting is: Automatically deny elevation requests.

Rationale: One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run.

CCE Reference Number: CCE-36864-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.17.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'User Account Control: Behavior of the elevation prompt for standard users' is set to 'Automatically deny elevation requests'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Automatically deny elevation requests:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Behavior of the elevation prompt for standard users>

Impact: When an operation requires elevation of privilege, a configurable access denied error message is displayed. An enterprise that is running desktops as standard user may choose this setting to reduce help desk calls.

Note: With this setting configured as recommended, the default error message displayed when a user attempts to perform an operation or run a program requiring privilege elevation (without Administrator rights) is "This program will not run. This program is blocked by group policy. For more information, contact your system administrator." Some users who are not used to seeing this message may believe that the operation or program they attempted is specifically blocked by group policy, as that is what the message seems to imply. This message may therefore result in user questions as to why that specific operation/program is blocked, when in fact, the problem is that they need to perform the operation or run the program with an Administrative account (or "Run as Administrator" if it is already an Administrator account), and they are not doing that.

Vulnerability Details

This policy setting controls the behavior of the elevation prompt for standard users. The recommended state for this setting is: Automatically deny elevation requests.

Rationale: One of the risks that the User Account Control feature introduced with Windows Vista is trying to mitigate is that of malicious programs running under elevated credentials without the user or administrator being aware of their activity. This setting raises awareness to the user that a program requires the use of elevated privilege operations and requires that the user be able to supply administrative credentials in order for the program to run.

CCE Reference Number: CCE-36864-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.17.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting controls the behavior of application installation detection for the computer. The options are:- Enabled: (Default for home) When an application installation package is detected that requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.- Disabled: (Default for enterprise) Application installation packages are not detected and prompted for elevation. Enterprises that are running standard user desktops and use delegated installation technologies such as Group Policy Software Installation or Systems Management Server (SMS) should disable this policy setting. In this case, installer detection is unnecessary. The recommended state for this setting is: Enabled.

Rationale: Some malicious software will attempt to install itself after being given permission to run. For example, malicious software with a trusted application shell. The user may have given permission for the program to run because the program is trusted, but if they are then prompted for installation of an unknown component this provides another way of trapping the software before it can do damage

CCE Reference Number: CCE-36533-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.17.5

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation Impact: Users will need to provide administrative passwords to be able to install programs.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Detect application installations and prompt for elevation' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Detect application installations and prompt for elevation>

Impact: When an application installation package is detected that requires elevation of privilege, the user is prompted to enter an administrative user name and password. If the user enters valid credentials, the operation continues with the applicable privilege.

Vulnerability Details

This policy setting controls the behavior of application installation detection for the computer. The recommended state for this setting is: Enabled.

Rationale: Some malicious software will attempt to install itself after being given permission to run. For example, malicious software with a trusted application shell. The user may have given permission for the program to run because the program is trusted, but if they are then prompted for installation of an unknown component this provides another way of trapping the software before it can do damage

CCE Reference Number: CCE-36533-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.17.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following:- #x2026;\Program Files\, including subfolders- #x2026;\Windows\system32\- #x2026;\Program Files (x86)\, including subfolders for 64-bit versions of Windows Note: Windows enforces a public key infrastructure (PKI) signature check on any interactive application that requests to run with a UIAccess integrity level regardless of the state of this security setting. The options are:- Enabled: (Default) If an application resides in a secure location in the file system, it runs only with

UIAccess integrity.- Disabled: An application runs with UIAccess integrity even if it does not reside in a secure location in the file system. The recommended state for this setting is: Enabled.

Rationale: UIAccess Integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when an application is elevated in privilege from a standard user to an administrator. This is required to support accessibility features such as screen readers that are transmitting user interfaces to alternative forms. A process that is started with UIAccess rights has the following abilities:- To set the foreground window.- To drive any application window using SendInput function.- To use read input for all integrity levels using low-level hooks, raw input, GetKeyState, GetAsyncKeyState, and GetKeyboardInput.- To set journal hooks.- To uses AttachThreadInput to attach a thread to a higher integrity input queue.

CCE Reference Number: CCE-37057-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.17.6

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations Impact: If the application that requests UIAccess meets the UI Access setting requirements, Windows Vista starts the application with the ability to bypass most of the UIPI restrictions. If the application does not meet the security restrictions, the application will be started without UIAccess rights and can interact only with applications at the same or lower privilege level.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Only elevate UIAccess applications that are installed in secure locations' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting controls whether applications that request to run with a User Interface Accessibility (UIAccess) integrity level must reside in a secure location in the file system. Secure locations are limited to the following: - \Program Files\, including subfolders - \Windows\system32\ - \Program Files (x86)\, including subfolders for 64-bit versions of Windows.

Note: Windows enforces a public key infrastructure (PKI) signature check on any interactive application that requests to run with a UIAccess integrity level regardless of the state of this security setting. The recommended state for this setting is: Enabled.

Rationale: UIAccess Integrity allows an application to bypass User Interface Privilege Isolation (UIPI) restrictions when an application is elevated in privilege from a standard user to an administrator. This is required to support accessibility features such as screen readers that are transmitting user interfaces to alternative forms. A process that is started with UIAccess rights has the following abilities: - To set the foreground window. - To drive any application window using SendInput function. - To use read input for all integrity levels using low-level hooks, raw input, GetKeyState, GetAsyncKeyState, and GetKeyboardInput. - To set journal hooks. - To uses AttachThreadInput to attach a thread to a higher integrity input queue.

CCE Reference Number: CCE-37057-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.17.6

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Only elevate UIAccess applications that are installed in secure locations>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode Impact: Users and administrators will need to learn to work with UAC prompts and adjust their work habits to use least privilege operations.

Vulnerability Details

This policy setting controls the behavior of all User Account Control (UAC) policy settings for the computer. If you change this policy setting, you must restart your computer. The options are:- Enabled: (Default) Admin Approval Mode is enabled. This policy must be enabled and related UAC policy settings must also be set appropriately to allow the built-in Administrator account and all other users who are members of the Administrators group to run in Admin Approval Mode.- Disabled: Admin Approval Mode and all related UAC policy settings are disabled.

Note: If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced. The recommended state for this setting is: Enabled.

Rationale: This is the setting that turns on or off UAC. If this setting is disabled, UAC will not be used and any security benefits and risk mitigations that are dependent on UAC will not be present on the system.

CCE Reference Number: CCE-36869-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.17.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Run all administrators in Admin Approval Mode' is set to 'Enabled' — Trivial

Vulnerability Details

This policy setting controls the behavior of all User Account Control (UAC) policy settings for the computer. If you change this policy setting, you must restart your computer. The recommended state for this setting is: Enabled.

Note: If this policy setting is disabled, the Security Center notifies you that the overall security of the operating system has been reduced.

Rationale: This is the setting that turns on or off UAC. If this setting is disabled, UAC will not be used and any security benefits and risk mitigations that are dependent on UAC will not be present on the system.

CCE Reference Number: CCE-36869-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.17.7

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Run all administrators in Admin Approval Mode>

Impact: None - this is the default configuration. Users and administrators will need to learn to work with UAC prompts and adjust their work habits to use least privilege operations.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'

Trivial

Vulnerability Details

This policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop. The options are:- Enabled: (Default) All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users.- Disabled: All elevation requests go to the interactive user's desktop. Prompt behavior policy settings for administrators and standard users are used. The recommended state for this setting is: Enabled.

Rationale: Elevation prompt dialog boxes can be spoofed, causing users to disclose their passwords to malicious software.

CCE Reference Number: CCE-36866-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.17.8

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation Impact: None. This is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Switch to the secure desktop when prompting for elevation' is set to 'Enabled'	Trivial

Vulnerability Details

This policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop. The recommended state for this setting is: Enabled.

Rationale: Standard elevation prompt dialog boxes can be spoofed, which may cause users to disclose their passwords to malicious software. The secure desktop presents a very distinct appearance when prompting for elevation, where the user desktop dims, and the elevation prompt UI is more prominent. This increases the likelihood that users who become accustomed to the secure desktop will recognize a spoofed elevation prompt dialog box and not fall for the trick.

CCE Reference Number: CCE-36866-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.17.8

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Switch to the secure desktop when prompting for elevation>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'	Trivial

Vulnerability Details

This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to %ProgramFiles%, %Windir%, %Windir%\system32, or HKEY_LOCAL_MACHINE\Software. The options are:- Enabled: (Default) Application write failures are redirected at run time to defined user locations for both the file system and registry.- Disabled: Applications that write data to protected locations fail. The recommended state for this setting is:

Enabled.

Rationale: This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

CCE Reference Number: CCE-37064-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 2.3.17.9

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations Impact: None. This is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'User Account Control: Virtualize file and registry write failures to per-user locations' is set to 'Enabled'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Enabled:

<Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\User Account Control: Virtualize file and registry write failures to per-user locations>

Impact: None - this is the default configuration.

Vulnerability Details

This policy setting controls whether application write failures are redirected to defined registry and file system locations. This policy setting mitigates applications that run as administrator and write run-time application data to: - %ProgramFiles%, - %Windir%, - %Windir%\system32, or - HKEY_LOCAL_MACHINE\Software. The recommended state for this setting is: Enabled.

Rationale: This setting reduces vulnerabilities by ensuring that legacy applications only write data to permitted locations.

CCE Reference Number: CCE-37064-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 2.3.17.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\WDigest Authentication (disabling may require KB2871997)

Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).
Impact: None - this is the default behavior for Windows 8.1 and Server 2012 R2.

Vulnerability Details

When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about UseLogonCredential, see Microsoft Knowledge Base article 2871997: Microsoft Security Advisory Update to improve credentials protection and management May 13, 2014. The recommended state for this setting is: Disabled.

Rationale: Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

CCE Reference Number: CCE-38444-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 18.6.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'WDigest Authentication' is set to 'Disabled' — Trivial

Vulnerability Details

When WDigest authentication is enabled, Lsass.exe retains a copy of the user's plaintext password in memory, where it can be at risk of theft. If this setting is not configured, WDigest authentication is disabled in Windows 8.1 and in Windows Server 2012 R2; it is enabled by default in earlier versions of Windows and Windows Server. For more information about local accounts and credential theft, review the "Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques" documents. For more information about UseLogonCredential, see Microsoft Knowledge Base article 2871997: Microsoft Security Advisory Update to improve credentials protection and management May 13, 2014. The recommended state for this setting is: Disabled.

Rationale: Preventing the plaintext storage of credentials in memory may reduce opportunity for credential theft.

CCE Reference Number: CCE-38444-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.6.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Disabled: Computer Configuration\Policies\Administrative Templates\SCM: Pass the Hash Mitigations\WDigest Authentication (disabling may require KB2871997)

Note: This Group Policy path does not exist by default. An additional Group Policy template (PtH.admx/adml) is required - it is included with Microsoft Security Compliance Manager (SCM).
Impact: None - this is the default configuration for Windows 8.1 and Server 2012 R2.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Firewall state Impact: None, this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended).

Rationale: If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-36062-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.1

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Firewall state' is set to 'On (recommended)'	**Trivial**

Solution Details

To establish the recommended configuration via GP, set the following UI path to On (recommended):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Firewall state>

Impact: None - this is the default configuration.

Vulnerability Details

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended).

Rationale: If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-36062-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)' — Trivial

Vulnerability Details

This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default).

Rationale: If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-38117-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Block (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Inbound connections Impact: None, this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Inbound connections' is set to 'Block (default)'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Block (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Inbound connections>

Impact: None - this is the default configuration.

Vulnerability Details

This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The recommended state for this setting is: Block (default).

Rationale: If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-38117-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37523-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log dropped packets' is set to 'Yes'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log dropped packets>

Impact: Information about dropped packets will be recorded in the firewall log file.

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37523-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36393-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Logging: Log successful connections' is set to 'Yes' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Log successful connections>

Impact: Information about successful connections will be recorded in the firewall log file.

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36393-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewalldomainfw.log'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Vulnerability Details

Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37482-7
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.7

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\domainfw.log'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Name>

Impact: The log file will be stored in the specified file.

Vulnerability Details

Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37482-7
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Vulnerability Details

Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36088-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Logging Customize\Size limit (KB)>

Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36088-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.8

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'	Trivial

Vulnerability Details

This setting determines the behavior for outbound connections that do not match an outbound firewall rule. In Windows Vista / Server 2008 and above, the default behavior is to allow connections unless there are firewall rules that block the connection. The recommended state for this setting is: Allow (default).

Rationale: Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

CCE Reference Number: CCE-36146-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Outbound connections Impact: None, this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Outbound connections' is set to 'Allow (default)'

Trivial

Vulnerability Details

This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The recommended state for this setting is: Allow (default).

Rationale: Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

CCE Reference Number: CCE-36146-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Allow (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Outbound connections>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Vulnerability Details

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default).

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-38040-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local connection security rules' is set to 'Yes (default)' Trivial

Vulnerability Details

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default).

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-38040-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.6

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Apply local connection security rules>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'

Trivial

Vulnerability Details

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default).

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-37860-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.5

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Settings: Apply local firewall rules' is set to 'Yes (default)'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Apply local firewall rules>

Impact: None - this is the default configuration.

Vulnerability Details

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default).

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-37860-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No: Computer

Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No.

Rationale: Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

CCE Reference Number: CCE-38041-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.1.4

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Domain: Settings: Display a notification' is set to 'No' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Domain Profile\Settings Customize\Display a notification>

Impact: Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Vulnerability Details

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. The recommended state for this setting is: No.

Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale: Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

CCE Reference Number: CCE-38041-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.1.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)' — Trivial

Vulnerability Details

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended).

Rationale: If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-38239-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Firewall state Impact: None, this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Firewall state' is set to 'On (recommended)'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to On (recommended):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Firewall state>

Impact: None - this is the default configuration.

Vulnerability Details

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended).

Rationale: If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-38239-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Block (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Inbound connections Impact: None, this is the default configuration.

Vulnerability Details

This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default).

Rationale: If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-38042-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Inbound connections' is set to 'Block (default)'

Trivial

Vulnerability Details

This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The recommended state for this setting is: Block (default).

Rationale: If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-38042-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Block (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Inbound connections>

Impact: None - this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-35972-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Logging: Log dropped packets' is set to 'Yes'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log dropped packets>

Impact: Information about dropped packets will be recorded in the firewall log file.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-35972-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.9

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37387-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.10

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Logging: Log successful connections' is set to 'Yes'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Log successful connections>

Impact: Information about successful connections will be recorded in the firewall log file.

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37387-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallprivatefw.log' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Vulnerability Details

Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is:
%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37569-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\privatefw.log' Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Name>

Impact: The log file will be stored in the specified file.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37569-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.7

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater' — Trivial

Vulnerability Details

Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-38178-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.8

Solution Details

To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Logging: Size limit (KB)' is set to '16,384 KB or greater'	Trivial

Vulnerability Details

Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-38178-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Logging Customize\Size limit (KB)>

Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)' — Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: Allow (default).

Rationale: Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

CCE Reference Number: CCE-38332-3
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Outbound connections Impact: None, this is the default configuration.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Outbound connections' is set to 'Allow (default)'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Allow (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Outbound connections>

Impact: None - this is the default configuration.

Vulnerability Details

This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The recommended state for this setting is: Allow (default).

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale: Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

CCE Reference Number: CCE-38332-3
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Vulnerability Details

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default).

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-36063-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local connection security rules' is set to 'Yes (default)'

Trivial

Vulnerability Details

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: Yes (default).

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-36063-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.6

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with

Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Apply local connection security rules>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Vulnerability Details

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default).

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-37438-9
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Windows Firewall: Private: Settings: Apply local firewall rules' is set to 'Yes (default)'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Apply local firewall rules>

Impact: None - this is the default configuration.

Vulnerability Details

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: Yes (default).

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-37438-9
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private

Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

Vulnerability Details

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored. The recommended state for this setting is: No.

Rationale: Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

CCE Reference Number: CCE-37621-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.2.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Private: Settings: Display a notification' is set to 'No' — Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to No:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Private Profile\Settings Customize\Display a notification>

Impact: Windows Firewall will not display a notification when a program is blocked from receiving inbound connections.

Vulnerability Details

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. The recommended state for this setting is: No.

Note: When the Apply local firewall rules setting is configured to No, it's recommended to also configure the Display a notification setting to No. Otherwise, users will continue to receive messages that ask if they want to unblock a restricted inbound connection, but the user's response will be ignored.

Rationale: Firewall notifications can be complex and may confuse the end users, who would not be able to address the alert.

CCE Reference Number: CCE-37621-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.2.4

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' | Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to On (recommended): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Firewall state Impact: None, this is the default configuration.

Vulnerability Details

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended).

Rationale: If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-37862-0
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Firewall state' is set to 'On (recommended)' — Trivial

Vulnerability Details

Select On (recommended) to have Windows Firewall with Advanced Security use the settings for this profile to filter network traffic. If you select Off, Windows Firewall with Advanced Security will not use any of the firewall rules or connection security rules for this profile. The recommended state for this setting is: On (recommended).

Rationale: If the firewall is turned off all traffic will be able to access the system and an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-37862-0
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.1

Solution Details

To establish the recommended configuration via GP, set the following UI path to On (recommended):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Firewall state>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Block (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Inbound connections Impact: None, this is the default configuration.

Vulnerability Details

This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The default behavior is to block connections unless there are firewall rules to allow the connection. The recommended state for this setting is: Block (default).

Rationale: If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-36057-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.2

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Inbound connections' is set to 'Block (default)' — Trivial

Vulnerability Details

This setting determines the behavior for inbound connections that do not match an inbound firewall rule. The recommended state for this setting is: Block (default).

Rationale: If the firewall allows all traffic to access the system then an attacker may be more easily able to remotely exploit a weakness in a network service.

CCE Reference Number: CCE-36057-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.2

Solution Details

To establish the recommended configuration via GP, set the following UI path to Block (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public

Profile\Inbound connections>

Impact: None - this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'

Trivial

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37265-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.9

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log dropped packets Impact: Information about dropped packets will be recorded in the firewall log file.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Logging: Log dropped packets' is set to 'Yes'	Trivial

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security discards an inbound packet for any reason. The log records why and when the packet was dropped. Look for entries with the word DROP in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37265-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.9

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log dropped packets>

Impact: Information about dropped packets will be recorded in the firewall log file.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'	Trivial

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36394-5
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Log successful connections Impact: Information about successful connections will be recorded in the firewall log file.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Logging: Log successful connections' is set to 'Yes'

Trivial

Vulnerability Details

Use this option to log when Windows Firewall with Advanced Security allows an inbound connection. The log records why and when the connection was formed. Look for entries with the word ALLOW in the action column of the log. The recommended state for this setting is: Yes.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36394-5
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.10

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public

Profile\Logging Customize\Log successful connections>

Impact: Information about successful connections will be recorded in the firewall log file.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%System32logfilesfirewallpublicfw.log'	Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Name Impact: The log file will be stored in the specified file.

Vulnerability Details

Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is: %SYSTEMROOT%\System32\logfiles\firewall\publicfw.log.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37266-4
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Logging: Name' is set to '%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log'	Trivial

Vulnerability Details

Use this option to specify the path and name of the file in which Windows Firewall will write its log information. The recommended state for this setting is:
%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-37266-4
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.7

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to
%SYSTEMROOT%\System32\logfiles\firewall\publicfw.log:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Name>

Impact: The log file will be stored in the specified file.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Size limit (KB) Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

Vulnerability Details

Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36395-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.8

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Logging: Size limit (KB)' is set to '16,384 KB or greater'

Trivial

Vulnerability Details

Use this option to specify the size limit of the file in which Windows Firewall will write its log information. The recommended state for this setting is: 16,384 KB or greater.

Rationale: If events are not recorded it may be difficult or impossible to determine the root cause of system problems or the unauthorized activities of malicious users.

CCE Reference Number: CCE-36395-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.8

Solution Details

To establish the recommended configuration via GP, set the following UI path to 16,384 KB or greater:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Logging Customize\Size limit (KB)>

Impact: The log file size will be limited to the specified size, old events will be overwritten by newer ones when the limit is reached.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'	Trivial

Vulnerability Details

This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The default behavior is to allow connections unless there are firewall rules that block the connection. Important: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying. The recommended state for this setting is: Allow (default).

Rationale: Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

CCE Reference Number: CCE-37434-8
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.3

Solution Details

To establish the recommended configuration via GP, set the following UI path to Allow (default): Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Outbound connections Impact: None, this is the default configuration.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Outbound connections' is set to 'Allow (default)'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Allow (default):

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Outbound connections>

Impact: None - this is the default configuration.

Vulnerability Details

This setting determines the behavior for outbound connections that do not match an outbound firewall rule. The recommended state for this setting is: Allow (default).

Note: If you set Outbound connections to Block and then deploy the firewall policy by using a GPO, computers that receive the GPO settings cannot receive subsequent Group Policy updates unless you create and deploy an outbound rule that enables Group Policy to work. Predefined rules for Core Networking include outbound rules that enable Group Policy to work. Ensure that these outbound rules are active, and thoroughly test firewall profiles before deploying.

Rationale: Some people believe that it is prudent to block all outbound connections except those specifically approved by the user or administrator. Microsoft disagrees with this opinion, blocking outbound connections by default will force users to deal with a large number of dialog boxes prompting them to authorize or block applications such as their web browser or instant messaging software. Additionally, blocking outbound traffic has little value because if an attacker has compromised the system they can reconfigure the firewall anyway.

CCE Reference Number: CCE-37434-8
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.3

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local connection security rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

Vulnerability Details

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: No.

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-36268-1
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local connection security rules' is set to 'No' — Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to No:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local connection security rules>

Impact: Administrators can still create local connection security rules, but the rules will not be applied.

Vulnerability Details

This setting controls whether local administrators are allowed to create connection security rules that apply together with connection security rules configured by Group Policy. The recommended state for this setting is: No.

Rationale: Users with administrative privileges might create firewall rules that expose the system to remote attack.

CCE Reference Number: CCE-36268-1
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.6

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'

Trivial

Vulnerability Details

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: No.

Rationale: When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

CCE Reference Number: CCE-37861-2
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.5

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

To establish the recommended configuration via GP, set the following UI path to No: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local firewall rules Impact: If you configure this setting to No, administrators can still create firewall rules, but the rules will not be applied. This setting is available only when configuring the policy through Group Policy.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Settings: Apply local firewall rules' is set to 'No'	Trivial

Vulnerability Details

This setting controls whether local administrators are allowed to create local firewall rules that apply together with firewall rules configured by Group Policy. The recommended state for this setting is: No.

Rationale: When in the Public profile, there should be no special local firewall exceptions per computer. These settings should be managed by a centralized policy.

CCE Reference Number: CCE-37861-2
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.5

Solution Details

To establish the recommended configuration via GP, set the following UI path to No:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Apply local firewall rules>

Impact: Administrators can still create firewall rules, but the rules will not be applied.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'	Trivial

Vulnerability Details

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections.

Note: When the Apply local firewall rules setting is configured to Yes, it is also recommended to also configure the Display a notification setting to Yes. Otherwise, users will not receive messages that ask if they want to unblock a restricted inbound connection. The recommended state for this setting is: Yes.

Rationale: Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

CCE Reference Number: CCE-38043-6
CIS_Microsoft_Windows_Server_2012_R2_Benchmark_v2.2.0: 9.3.4

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes: Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Display a notification Impact: If you configure this policy setting to No, Windows Firewall will not display these notifications.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Ensure 'Windows Firewall: Public: Settings: Display a notification' is set to 'Yes'

Trivial

Solution Details

To establish the recommended configuration via GP, set the following UI path to Yes:

<Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Windows Firewall Properties\Public Profile\Settings Customize\Display a notification>

Impact: None - this is the default configuration.

Vulnerability Details

Select this option to have Windows Firewall with Advanced Security display notifications to the user when a program is blocked from receiving inbound connections. The recommended state for this setting is: Yes.

Note: When the Apply local firewall rules setting is configured to Yes, it is also recommended to also configure the Display a notification setting to Yes. Otherwise, users will not receive messages that ask if they want to unblock a restricted inbound connection.

Rationale: Some organizations may prefer to avoid alarming users when firewall rules block certain types of network activity. However, notifications can be helpful when troubleshooting network issues involving the firewall.

CCE Reference Number: CCE-38043-6
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 9.3.4

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Compliance: Set 'NetBIOS node type' to 'P-node' (Ensure NetBT Parameter 'NodeType' is set to '0x2 (2)') (MS Only)

Trivial

Solution Details

To establish the recommended configuration, set the following Registry value to 0x2 (2) (DWORD):
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters:NodeType

Note: This change does not take effect until the computer has been restarted. Note #2: Although Microsoft does not provide an ADMX template to configure this registry value, a custom .ADM template (Set-NetBIOS-node-type-KB160177.adm) is provided in the CIS Benchmark Remediation Kit to facilitate its configuration. Be aware though that simply turning off the group policy setting in the .ADM template will not "undo" the change once applied. Instead, the opposite setting must be applied to change the registry value to the opposite state.

Impact: NetBIOS name resolution queries will require a defined and available WINS server for external NetBIOS name resolution. If a WINS server is not defined or not reachable, and the desired hostname is not defined in the local cache, local LMHOSTS or HOSTS files, NetBIOS name resolution will fail.

Vulnerability Details

This parameter determines which method NetBIOS over TCP/IP (NetBT) will use to register and resolve names. A B-node (broadcast) system only uses broadcasts. A P-node (point-to-point) system uses only name queries to a name server (WINS). An M-node (mixed) system broadcasts first, then queries the name server (WINS). An H-node (hybrid) system queries the name server (WINS) first, then broadcasts. The recommended state for this setting is: NodeType - 0x2 (2).

Rationale: In order to help mitigate the risk of NetBIOS Name Service (NBT-NS) poisoning attacks, setting the node type to P-node will prevent the system from sending out NetBIOS broadcasts.
CIS_Microsoft_Windows_Server_2016_Benchmark_v1.0.0: 18.4.4.1

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Content Security Policy Missing — Trivial

Solution Details

Add a Content Security Policy (CSP) based upon your specific needs. Please refer to the documentation on CSPs to configure the right policy.
Caveats:
Please note the inclusion of a Content Security Policy (CSP) does not replace good security hygiene. Using a CSP to block known Cross-site Scripting (XSS) vulnerabilities (for example) is not recommended.

Vulnerability Details

Not having a Content-Security-Policy (CSP) potentially opens a website to vulnerabilities such as, but not limited to: cross-site scripting (XSS), clickjacking and other code injection attacks resulting from the execution of malicious content in the trusted web page context.

False Positive Notes

We are checking to see if either an html meta tag or "Content-Security-Policy" header is missing from an audited web-page. If the tag format or header name changes in the future. This could lead to a false positive.

CVSS Base Score: 2.6

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Type	Reference
URL	https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Daytime Service Detected — Trivial

Solution Details

The daytime service is an inessential service which can safely be disabled without experiencing adverse consequences in other network or program functionality. The following are instructions for disabling the daytime service on a system:

Unix/Linux with inetd: Comment out 'daytime' in the /etc/inetd.conf file and restart inetd.

Unix with xinetd: Change directory to the xinetd daemon directory (typically /etc/xinetd.d, as defined in the xinetd.conf file), and edit the daytime and daytime-udp files (if they exist) and either change the existing line 'disable' to 'disable = yes' or add the line between the curly braces if it does not exist. If individual configuration files are not used for each service, edit the xinetd.conf file and follow the same instructions for each instance of the 'daytime' service. Restart the xinetd service after all changes have been saved.

Windows: Remove the Simple TCP/IP Services from the network configuration.

Cisco: At the enable console, in configuration mode, enter 'no service tcp-small-servers' and 'no service udp-small-servers'.

Others: Consult the system documentation.
Caveats:
Disabling the Simple TCP/IP Services on Windows will also disable Character Generator, Discard, Echo, and Quote of the Day.
Workarounds:
Restrict access to TCP/UDP port 13 via host or network based firewall rules to authorized hosts only.

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

Vulnerability Details

The host is running the daytime service. The daytime service is a debugging tool which listens on a port for incoming packets and responds with a packet containing a date and time.
Impact:
The format of the date that is issued by the daytime service may help an attacker guess the operating system type of the system which is running the service. Additionally, the UDP version of daytime service can be leveraged by an attacker to flood the server via a "UDP bomb" or "packet storm", resulting in a denial-of-service condition on the vulnerable host.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0103
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-233-01
URL	http://tools.ietf.org/html/rfc867
URL	http://www.faqs.org/rfcs/rfc867.html
URL	http://www.cert.org/advisories/CA-1996-01.html

Default Apache Tomcat Webpage Detected | Trivial

Solution Details

Please ensure this host is configured to appropriately restrict access.

Vulnerability Details

This host is running an Apache Tomcat web server. The default Apache Tomcat "It Works!" page implies this host may not be configured for optimal security.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Default IIS Webpage Detected | Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This host is running Microsoft's IIS webserver. The default webpage that has been detected on this host implies this host may not be configured for optimal security. An attacker can leverage this to gain access to or information about this host.

Solution Details

Please ensure this host is configured to appropriately restrict access

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Discard Service Detected | Trivial

Solution Details

The discard service is an inessential service which can safely be disabled without experiencing adverse consequences in other network or program functionality. The following are instructions for disabling the discard service on a system:

Unix/Linux with inetd: Comment out 'discard' in the /etc/inetd.conf file and restart inetd.

Unix with xinetd: Change directory to the xinetd daemon directory (typically /etc/xinetd.d, as defined in the xinetd.conf file), and edit the discard and discard-udp files (if they exist) and either change the existing line 'disable' to 'disable = yes' or add the line between the curly braces if it does not exist. If individual configuration files are not used for each service, edit the xinetd.conf file and follow the same instructions for each instance of the 'discard' service. Restart the xinetd service after all changes have been saved.

Windows: Remove the Simple TCP/IP Services from the network configuration.

Cisco: At the enable console, in configuration mode, enter 'no service tcp-small-servers' and 'no service udp-small-servers'.

Others: Consult the system documentation.
Caveats:
Disabling the Simple TCP/IP Services on Windows will also disable Character Generator, Daytime, Echo, and Quote of the Day.
Workarounds:
Restrict access to TCP/UDP port 9 via host or network based firewall rules to authorized hosts only.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The host is running the discard service. The discard service is a network debugging tool used for testing and measurement as defined by RFC 863. When the discard service receives a packet, it immediately throws the packet away without sending a response to the client.
Impact:
The presence of the discard service has little to no impact to the security of this host. However, exposing any service which is not specifically used for business purposes needlessly increases the attack surface (aka the potential for attack) for a given host.
Caveats:
The discard service is similar to /dev/null on a Unix/Linux host and will immediately and silently throw away all data that it receives. Because the service throws away data without sending a response, the vulnerability check identifies the discard service only based on the presence of TCP or UDP port 9.

CVSS Base Score: 10

CVSS Vector: AV:N/AC:L/Au:N/C:C/I:C/A:C

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0636
URL	http://tools.ietf.org/html/rfc863

Type	Reference
URL	http://en.wikipedia.org/wiki/DISCARD

Echo Service | Trivial

Vulnerability Details

The echo service is a simple network service which responds to incoming packets with an exact duplicate, or echo, of the packet. It is possible for an attacker to leverage the echo service in order to cause a denial-of-service condition.
Impact:
An attacker can utilize all of a system's resources by continually requesting responses from the echo service. The impact of this attack will vary depending on the purpose of the victim machine. Client-facing, internet-accessible systems have a higher liability than user workstations.

Solution Details

The echo service is intended for testing purposes only and can safely be disabled without experiencing adverse behavior on the network.

Disable the echo service on the vulnerable host by following the appropriate instructions for the affected system.

Unix: Comment out 'echo' in the /etc/inetd.conf file and restart inetd.
Windows: Remove the Simple TCP/IP Services from the network configuration.
Cisco: At the enable console, in configuration mode, enter 'no service tcp-small-servers' and 'no service udp-small-servers'.
Others: Consult the system documentation.

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0635
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0103
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-233-01
URL	http://www.cert.org/advisories/CA-1996-01.html

HTTP TRACE/TRACK Method Enabled | Trivial

Solution Details

The HTTP TRACE/TRACK method was designed for debugging and diagnostic purposes. Consider disabling HTTP TRACE/TRACK support in the web server if it is unnecessary.

Apache web servers:
Use the Apache mod_rewrite module to deny HTTP TRACE/TRACK requests or to permit only the methods needed to meet site requirements and policy. A basic example of this is to use the following in the httpd configuration file. This must be defined in each virtual host if virtual hosting is used:

```
RewriteEngine On
RewriteCond % ^TRACE
RewriteRul: .* - [F]
```

Windows 2003 Server users:
Download the WinHttpTraceCfg.exe from http://msdn.microsoft.com/en-us/library/aa384119%28VS.85%29.aspx.

Windows IIS web server users:
Install URLScan tool from http://technet.microsoft.com/en-us/security/cc242650.aspx.

Default Configuration of URL Scan will only allow GET, HEAD, and POST
Advanced Configuration of URLScan is available at the Microsoft library article cc242650 linked above.

1. Navigate to %windir%\system32\inetsrv\urlscan
2. Edit urlscan.ini
3. Configure as desired

Restart IIS
1. Navigate to Administrative Tools
2. Open Internet Information Services
3. Right Click on desired web server
4. Select All Tasks -> Restart IIS

Windows IIS with Citrix NFuse:
This solution from Microsoft will not work on hosts running Citrix NFuse, and will force a complete system reload if applied to systems running Citrix NFuse.

For other types of web servers, please contact the vendor or consult the host documentation for further information.

Vulnerability Details

The TRACE/TRACK method of the Hypertext Transfer Protocol (HTTP) is defined to return the contents of client HTTP requests in the entity-body of the TRACE/TRACK response. The TRACK method is an alias of the TRACE method on certain servers. These methods are generally enabled for debugging purposes, and when enabled, can be leveraged by attackers to access sensitive information, such as cookies or authentication data, which is contained in the HTTP headers of the request and that are not otherwise available via the DOM interface. In the presence of other cross-site domain vulnerabilities in web browsers, sensitive header information can be read from domains other than the target of the HTTP TRACE/TRACK request.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.8

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2003-1567
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2320
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-0386
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2004-2763
BUGTRAQ	http://www.securityfocus.com/bid/9506
URL	http://msdn2.microsoft.com/en-us/library/aa302368.aspx
URL	http://www.aqtronix.com/Advisories/AQ-2003-02.txt
URL	http://technet.microsoft.com/en-us/security/cc242650.aspx
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
URL	http://msdn.microsoft.com/en-us/library/aa384119%28VS.85%29.aspx
URL	http://www.ietf.org/rfc/rfc2616.txt
URL	https://cwe.mitre.org/data/definitions/16.html
URL	http://msdn2.microsoft.com/en-us/library/aa384119.aspx

ICMP Timestamp Request — Trivial

Solution Details

Use access control to block incoming ICMP timestamp requests (ICMP 13), and outgoing ICMP timestamp replies (ICMP 14).

Vulnerability Details

Internet Control Message Protocol (ICMP) is an integral component of Internet Protocol (IP) implementations and is defined in IETF RFC 792. ICMP messages are used to support diagnostic and error reporting when problems are encountered by IP datagrams.

The ICMP RFC specifies a timestamp request and response which divulges the current date and time that is being used by the target host. Unfortunately, some programs and operating systems use the current time to generate pseudo random numbers that are used for encryption, session state, or other purposes. An attacker can use the response to an ICMP timestamp request to aid in defeating weak authentication systems that rely on this information.

Impact:
An attacker that is able to use the ICMP timestamp information from a vulnerable system to compromise a cryptographic system or authentication scheme will be able to gain access to the vulnerable system. This level of access differs greatly on a case by case basis.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.1

CVSS Vector: AV:L/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0524
URL	http://kb.vmware.com/selfservice/microsites/search.do?cmd=displayKC&externalId=1434
URL	http://www.ietf.org/rfc/rfc792.txt
URL	http://descriptions.securescout.com/tc/11011
URL	https://cwe.mitre.org/data/definitions/200.html
URL	http://descriptions.securescout.com/tc/11010

IPv6 Enabled — Trivial

Vulnerability Details

This asset has IPv6 enabled. If IPv6 is not being used by the asset, it should be disabled.
Impact:
An attacker can exploit IPv6 in Windows networks to spoof DNS replies by acting as a malicious DNS server and redirect traffic to an attacker specified endpoint. The attacker could then relay credentials and authenticate to other services within the network.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

IPv6 can be disabled on specific network interfaces via the following steps.

1. Open Network and Sharing Center via the Control Panel.
2. Choose "Change adapter settings"
3. Right-click and choose "Properties" for the desired network adapter.
4. Scroll down and uncheck the box for "Internet Protocol Version 6 (TCP/IPv6)".
5. Click 'OK'. No restart is required.

IPv6 can also be disabled on all interfaces by creating and setting a registry key.

Key: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
Value: DisabledComponents = ff
Value Type: DWORD (Hexadecimal value)

This method does require a system restart. For reference, the checkboxes mentioned above will remain checked even if the registry key option is implemented.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://docs.microsoft.com/en-us/troubleshoot/windows-server/networking/configure-ipv6-in-windows

Kerberos User Enumeration Detected | Trivial

Solution Details

This is a feature of the Kerberos protocol, therefore the only way to prevent it from being used for user enumeration is to restrict access to the Kerberos port on this host. However, this would also prevent legitimate use of the service.

Vulnerability Details

The Kerberos service can be used to determine if a user is enabled, disabled, or does not exist based on responses to AS-REQ Kerberos packets.
Impact:
If the domain of a Kerberos service is known, an unauthenticated remote attacker can enumerate the users of that domain to help with further attacks.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Link Local Multicast Name Resolution (LLMNR) Enabled | Trivial

Vulnerability Details

The Link Local Multicast Name Resolution (LLMNR) protocol is enabled on this asset. Thus, this asset will make LLMNR broadcasts to resolve hostnames on the local subnet.
Impact:
An attacker could potentially spoof LLMNR responses in order to obtain NTLMv2 credentials meant for a legitimate host.

Solution Details

The LLMNR protocol can be disabled by setting either of the following registry values to 0. If this value name does not exist, it can be created by adding a new DWORD value name and setting it to 0.
Note: If the key does not even exist, a new key may have to be added as well.

1.) Key/value
HKEY_LOCAL_MACHINE\Software\policies\Microsoft\Windows NT\DNSClient > EnableMulticast=0

2.) Key/value
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Dnscache\Parameters > EnableMulticast=0

The default behavior is for LLMNR multicast to be enabled if nothing is modified.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference

There are no references for this vulnerability.

Microsoft RDP Network Level Authentication Disabled | Trivial

Solution Details

Consider enabling Network Level Authentication.

Vulnerability Details

This asset appears to be running a Microsoft RDP service without Network Level Authentication (NLA) enabled.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

NetBIOS Over TCP/IP Enabled — Trivial

Vulnerability Details

The NetBIOS service is enabled on this asset. This means that this asset will initiate NetBIOS broadcasts and queries. Additionally, this asset will respond to NetBIOS requests made by other assets on this network.
Impact:
It may be possible for an attacker to spoof other assets on the network by responding to the NetBIOS requests.

Solution Details

Disable NetBIOS over TCP/IP.

NetBIOS over TCP/IP can be disabled by setting the following registry key value to 2. If the key does not exist, by default NetBIOS over TCP/IP is enabled, it can be created:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\NetBT\Parameters\Interfaces\<Interface GUID>\NetbiosOptions

This registry key value is of type DWORD.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

NTLM Authentication Host Information Disclosure

Trivial

Vulnerability Details

This service supports NTLM authentication. When sending a blank NTLM type 1 message, the server will respond with a NTLM type 2 message that contains the Active Directory domain, NetBIOS hostname, DNS hostname and DNS domain name for the host.
Impact:
Attackers can use this to discover the Active Directory domain and use it in further attacks against the network, such as brute forcing user logins for an Outlook Web Access server.

Solution Details

As the detection of the domain and host information is a feature of the NTLM authentication protocol, it is not a vulnerability. Therefore, no solution is required.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://technet.microsoft.com/en-us/library/jj865680(v=ws.10).aspx

Remote Desktop Protocol Allows Man in the Middle

Trivial

Vulnerability Details

This host is running Microsoft's Remote Desktop Protocol (RDP) server, formerly known as Microsoft's Terminal Services, for remote GUI administration of this host. The current configuration of this host's RDP server is vulnerable to a man-in-the-middle attack. The vulnerability arises due to the fact that the private key used to sign the RDP server's public key is hardcoded into mstlsapi.dll. This library is available publicly and can be used by an attacker to calculate the valid signature required to perform a man-in-the-middle attack. Note that this vulnerability exists even when native RDP encryption is being used between the RDP client and RDP server.
Impact:
An attacker that has successfully performed the man-in-the-middle attack could gain sensitive information including keystrokes sent from the RDP client to the RDP server. Tools such as Cain and Abel not only perform this attack but also attempt to automatically extract passwords typed in during RDP sessions.
Caveats:
An RDP server that allows Negotiate instead of requiring TLS/SSL may also be vulnerable because the attacker could force an RDP session to use RDP native encryption. This caveat is predicated on the RDP client's configuration also allowing native RDP encryption in place of requiring TLS/SSL.

Solution Details

Ensure that the RDP server is configured to require TLS/SSL encryption and authentication. For more information on configuring Microsoft's RDP server, please consult Microsoft's documentation for the specific version of the RDP server running on this host.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 6.4

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-1794
BUGTRAQ	http://www.securityfocus.com/bid/13818
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02

RPC Portmap Service — Trivial

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

Solution Details

Please disable this service if it is not in use. For Internet-facing systems, filter TCP and UDP port 111 inbound. Solaris systems should also filter TCP and UDP port 32771. If this service is required, please ensure the libc/glibc library has been patched against the XDR integer overflow vulnerabilities, and this host is running the latest version of RPC portmap linked in the References List of the vulnerability details section.

Vulnerability Details

This host is running the RPC 'portmap' service vulnerable to subversion. The portmapper acts as a directory service for locating RPC applications on this host, typically port 111. Attackers can leverage this service by sending UDP requests to rpcbind listening above port 32770 to determine if a vulnerable RPC application is running on this host.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0189
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0632

SMB Domain SID Disclosure

Trivial

Vulnerability Details

This host divulges the Windows domain SID through a NULL session. An attacker could use this SID to enumerate domain users in conjunction with the LookupAccountSid or LookupAccountName functions.

Solution Details

Upgrade the Windows OS and disable anonymous access to this host. If the host does not need to participate on a Windows network (file/printer sharing, RPC, DCOM, Remote Registry access, etc.), the Server service can safely be disabled. For more information, see the Microsoft Knowledge Article linked in the References List of the vulnerability details. If this host is accessible externally, filtering access to TCP ports 135, 138, 139, and 445 as well as UDP ports 137, 138, and 139 is recommended.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2000-1200
URL	http://support.microsoft.com/kb/143474

SMB Native LanMan Version

Trivial

Vulnerability Details

Lan Manager was originally developed in the 1980's as a network operating system by Microsoft in conjunction with other vendors such as IBM and 3COM. Since then, the Lan Manager has been evolved by Microsoft into the NT Lan Manager and is heavily used in Windows networking. This vulnerability check collects and displays information obtained from the Lan Manager including Lan Manager version, OS, and domain.
Impact:
Information provided by the Lan Manager can be used to fingerprint specific details about this host including its OS and domain. This information is not an information leak but rather specifically provided for Lan Manager functionality.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

No solution is required.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	http://en.wikipedia.org/wiki/LAN_Manager
URL	http://en.wikipedia.org/wiki/NTLM

SMB Null Session Authentication — Trivial

Solution Details

Please note the below settings will NOT remediate the "SMB NULL Session" vulnerability; it will only prevent an attacker from obtaining sensitive information via the NULL session.

To configure local security policy settings, open the Local Security Policy editor within the Administrative Tools and select SecuritySettings\Local Policies\SecurityOptions. Several options exist which pertain to SMB NULL sessions:

1. Network access: Allow anonymous SID/Name translation
2. Network access: Do not allow anonymous enumeration of SAM accounts
3. Network access: Do not allow anonymous enumeration of SAM accounts and shares
4. Network access: Let Everyone permissions apply to anonymous users
5. Network access: Named Pipes that can be accessed anonymously
6. Network access: Shares that can be accessed anonymously

To fully lock down SMB NULL session access, disable items 1 and 4, enable items 2 and 3, and set items 5 and 6 to an empty list. For detailed option information and security implications concerning the options listed above, refer to Microsoft's Threats and Countermeasures Guide for Security Options located at the URL http://technet.microsoft.com/en-us/library/dd349805(v=ws.10).

Vulnerability Details

This host is participating in a Windows-based network and allows NULL SMB sessions to be established. A NULL SMB session is an anonymous connection from one computer to another (usually both Windows computers) using the Windows Server Message Block (SMB) protocol.

SMB, also known as CIFS, is typically used for sharing resources on a network including files and printers. SMB also provides a robust inter-process communication (IPC) layer to allow processes to authenticate and communicate with each other either locally or over the network.
Impact:
An intruder can attach to the IPC$ (interprocess communications) share and gain information about the host, such as usernames, running services, and available NetBIOS shares. The actual level of information exposed depends on the security settings of this host.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 7.5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:P/A:P

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0520
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-1999-0519
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2002-1117
URL	https://msdn.microsoft.com/en-us/library/ms913275(v=winembedded.5).aspx
URL	http://support.microsoft.com/kb/314984

SSL Certificate: Chain Contains Weak RSA Keys — Trivial

Solution Details

Obtain a new SSL Certificate with a public key size greater then or equal to 2048 bits from a trusted Certificate Authority.

Vulnerability Details

The SSL Certificate running on this service appears to have been generated with a public key algorithm with a weak key size. SSL Certificate best practices recommends that RSA key sizes of at least 2048 bits are used when generating an SSL Certificate.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 2.6

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Type	Reference
URL	http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
URL	https://cwe.mitre.org/data/definitions/310.html
URL	http://www.symantec.com/page.jsp?id=1024-bit-migration-faq

SSL Certificate: Expired Certificate Date — Trivial

Solution Details

Please contact the certificate authority which issued the existing SSL certificate to obtain an updated version.

Vulnerability Details

This SSL Certificate's date has expired. Customers connecting to this website will now receive a warning stating that the SSL certificate to this site is not valid, breaking the chain-of-trust model that provides the rational behind SSL certificates. Users may become accustomed to clicking through the warning message making them more susceptible to phishing attacks carried out within the context of this website.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://cwe.mitre.org/data/definitions/324.html

SSL Certificate: Outdated Version — Trivial

Solution Details

Obtain a Version 3 SSL Certificate from a trusted Certificate Authority for this service.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The SSL Certificate that is presented by this service uses an outdated certificate version. SSL Certificate versions prior to version 3 are not considered to be cryptographically strong and are no longer acceptable for public use.

Impact:
SSL Certificates represent a method for clients of a service to trust that the remote server or service is actually the party it claims to be. Using a deprecated version of SSL Certificate, can make it difficult for clients of the service to trust that communication is occurring with the intended recipient.

Trusting remote services can be especially important if the service which is being accessed is a login page, an advisory page, etc. Using a deprecated SSL Certificate version makes the service vulnerable to attack by other parties who can now masquerade as the legitimate service more easily. The impact of an attack on this type of vulnerability includes that false information can be propagated as legitimate, that credentials be given to an attacker, or that legitimate users can be susceptible to other, more creative attacks.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

SSL Certificate: Weak Signature Algorithm SHA-1 — Trivial

Solution Details

Obtain a new SSL Certificate which is signed with a stronger hashing algorithm like SHA-2 from a trusted Certificate Authority. Cisco has released an update to address this issue which is available through the vendor link in the References List. Microsoft has also released an update to address this issue which is available through the vendor link in the References List.

Vulnerability Details

The SSL Certificate running on this service was signed with the SHA-1 hashing algorithm. For a stronger alternative to the SHA-1 hashing algorithm, utilize SHA-2 hashing algorithms (otherwise known as SHA-224, SHA-256, SHA-384 and SHA-512). NIST currently encourages all entities to move towards using SHA-2 family hashing algorithms over SHA-1. Additionally, standards such as PCI-DSS reference NIST as a guideline for preferring SHA-2 over SHA-1.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 5.9

CVSS Vector: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2005-4900
BUGTRAQ	http://www.securityfocus.com/bid/12577
URL	https://sites.google.com/site/itstheshappening
URL	https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html
URL	http://www.schneier.com/blog/archives/2005/02/sha1_broken.html
URL	http://www.cwi.nl/news/2017/cwi-and-google-announce-first-collision-industry-security-standard-sha-1
URL	http://shattered.io/
URL	http://www.microsoft.com/technet/security/advisory/961509.mspx

Type	Reference
URL	https://arstechnica.com/security/2017/02/at-deaths-door-for-years-widely-used-sha1-function-is-now-dead/
URL	http://ia.cr/2007/474
URL	https://cwe.mitre.org/data/definitions/326.html
URL	https://www.schneier.com/blog/archives/2005/08/new_cryptanalyt.html
URL	https://www.schneier.com/blog/archives/2005/02/sha1_broken.html
URL	http://csrc.nist.gov/groups/ST/hash/statement.html
URL	http://www.cisco.com/warp/public/707/cisco-sr-20090115-md5.shtml
URL	https://security.googleblog.com/2015/12/an-update-on-sha-1-certificates-in.html

SSL Connection: Anonymous (non-authenticated) Key-Agreement Protocols Permitted

Trivial

Solution Details

Disable anonymous key exchange protocols.

The following items can be added to the Apache site configuration for the SSLCipherSuite directive: "!ADH" and "!AECDH"

Vulnerability Details

Keys used during the exchange for Anonymous Diffie-Hellman and Anonymous Elliptic Curve Diffie-Hellman protocols do not provide authentication. As a result, these protocols are vulnerable to Man-in-The-Middle (MiTM) attacks.
Impact:
An attacker in position to perform a Man-in-The-Middle (MiTM) attack could intercept and eavesdrop or modify traffic between the client and server using this key exchange protocol.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

SSL Connection: SSL/TLS Supports RC4 Ciphers — Trivial

Solution Details

Disable support for the RC4 cipher suites in favor of TLS 1.2 AES-GCM cipher suites. Consult your specific vendor documentation for more information.

Vulnerability Details

RC4 is a fast stream cipher that has seen increased use as a means of mitigating the BEAST attack against CBC mode ciphers. However, RC4 suffers from several bytes biases in the keystream that could allow an attacker to extract pieces of plaintext from a TLS/SSL session that uses the RC4 cipher.
Impact:
A successful attack against a TLS/SSL session that uses the RC4 cipher could result in a leak of a limited amount of plaintext such as user credentials.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-2566
BUGTRAQ	http://www.securityfocus.com/bid/58796
URL	http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf
URL	http://blog.cryptographyengineering.com/2013/03/attack-of-week-rc4-is-kind-of-broken-in.html
URL	http://www.isg.rhul.ac.uk/tls/
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05336888
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05289935
URL	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
URL	https://cwe.mitre.org/data/definitions/310.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html

Type	Reference
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2016-2881720.html
URL	http://www.mozilla.org/security/announce/2013/mfsa2013-103.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuapr2016v3-2985753.html
URL	http://my.opera.com/securitygroup/blog/2013/03/20/on-the-precariousness-of-rc4
URL	http://www.opera.com/security/advisory/1046
URL	http://www.opera.com/docs/changelogs/unified/1215/
URL	http://cr.yp.to/talks/2013.03.12/slides.pdf

SSL Connection: SSLv3/TLSv1 Supports CBC Mode Ciphers — Trivial

Vulnerability Details

The SSL/TLS endpoint supports encryption using block ciphers (such as AES and DES) that operate in Cipher-Block Chaining (CBC) mode.

SSL ciphers are cryptographic algorithms used for transmitting certificates, establishing session keys, performing authentication, etc. Ciphers that operate in CBC mode are cryptographically weaker than other non-CBC mode ciphers of similar bit strengths. Additionally, SSLv3.0 and TLSv1.0 use CBC mode in such a way that cause the entire encrypted session to share one CBC session which creates a particularly weak situation that is subject to eavesdropping attacks and plain text insertion attacks.

The "Vulnerability Data" section includes a line which states whether the "Browser Exploit Against SSL/TLS" (BEAST) has been mitigated. This is determined as follows:

1. BEAST not mitigated: all supported ciphers are CBC mode ciphers

The scanner was unable to connect to the remote server using a non-CBC mode cipher.

2. BEAST not mitigated: server ignores client order but prefers CBC mode
ciphers

The scanner provided the remote service with non-CBC and CBC mode ciphers with a preference for non-CBC mode ciphers, but the service still selected a CBC mode cipher.

3. BEAST not mitigated: server respects client cipher order

The scanner provided the remote service with CBC and non-CBC mode ciphers, with a preference for CBC mode ciphers, and the service selected a CBC mode cipher.

4. BEAST mitigated: server ignores client order and prefers non-CBC mode
ciphers

The scanner determined that the remote service attempts to mitigate BEAST by preferring non-CBC mode ciphers.
Impact:
The method for selecting the cipher which will be used during an SSL/TLS session is selected during initialization of the connection. Since the remote server supports ciphers that operate in CBC mode, a client is able to establish a connection using a cipher from this family. In this scenario, the communication stream is susceptible to cryptographic attacks.

Solution Details

Supporting ciphers which operate in cipher-block chaining (CBC) mode is not a vulnerability and does not necessarily require remediation.

The "Vulnerability Data" section includes a line which references the status of BEAST mitigation. BEAST stands for Browser Exploit Against SSL/TLS -- a client-side attack which exploits the weaknesses of ciphers that operate in CBC mode. The server can promote the security of clients by preferring ciphers which do not operate in CBC mode.

In order to mitigate the BEAST attack, the server should be configured to select any of the provided, and supported, non-CBC mode ciphers that the client offers during SSL/TLS negotiation, over the offered CBC mode ciphers. Implementing this behavior will allow continued operability of the server with many SSL/TLS clients, while providing a best effort towards mitigating attacks against CBC mode ciphers.

On Microsoft Windows based operating systems, SSL cipher list ordering may be changed through the group policy editor as follows:

1. Open a command prompt and type in gpedit.msc
2. Navigate to Computer Configuration -> Administrative Templates -> Network -> SSL Configuration Settings
3. Open the SSL Cipher Suite Order setting
4. Change the order of the ciphers and save

For Apache using mod_ssl, the SSLProxyCipherSuite directive may be used to change the cipher order. Apache can also use the SSLHonorCipherOrder and SSLCipherSuite directives to control cipher order as follows:

```
SSLHonorCipherOrder On
SSLCipherSuite RC4-SHA:HIGH:!ADH
```

In general, this configuration will be specific to the application using SSL. For specific SSL configuration instructions, consult the appropriate user manual for the application using SSL or contact the vendor

of the application for more information.
Caveats:
Some browser-side implementations of SSL v3.0 and TLS v1.0 block ciphers which operate in cipher-block chaining (CBC) mode are susceptible to a client-side attack through the browser. This attack is known as the Browser Exploit Against SSL/TLS (BEAST). Threat of attack through this vector can be lessened by preferring stream ciphers, such as RC4, over these CBC mode block ciphers.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 4.3

CVSS Vector: AV:N/AC:M/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2011-3389
BUGTRAQ	http://www.securityfocus.com/bid/49778
BUGTRAQ	http://www.securityfocus.com/bid/49388
MSB	http://technet.microsoft.com/security/bulletin/MS12-006
URL	https://bugzilla.redhat.com/show_bug.cgi?id=737506
URL	http://blog.mozilla.com/security/2011/09/27/attack-against-tls-protected-communications/
URL	http://www.oracle.com/technetwork/topics/security/cpujan2015-1972971.html
URL	http://packetstormsecurity.com/files/131271/VMware-Security-Advisory-2015-0003.html
URL	http://eprint.iacr.org/2004/111
URL	http://isc.sans.edu/diary/SSL+TLS+part+3+/11635
URL	http://eprint.iacr.org/2006/136
URL	http://downloads.asterisk.org/pub/security/AST-2016-001.html
URL	http://support.apple.com/kb/HT5001
URL	http://www.educatedguesswork.org/2011/09/security_impact_of_the_rizzodu.html
URL	http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
URL	http://support.apple.com/kb/HT5501

Type	Reference
URL	http://support.apple.com/kb/HT5130
URL	http://googlechromereleases.blogspot.com/2011/10/chrome-stable-release.html
URL	http://vnhacker.blogspot.com/2011/09/beast.html
URL	http://www.imperialviolet.org/2011/09/23/chromeandbeast.html
URL	http://curl.haxx.se/docs/adv_20120124B.html
URL	https://bugzilla.novell.com/show_bug.cgi?id=719047
URL	http://support.apple.com/kb/HT6150
URL	https://blogs.oracle.com/sunsecurity/entry/multiple_vulnerabilities_in_fetchmail
URL	http://www.oracle.com/technetwork/topics/security/javacpuoct2011-443431.html
URL	http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslproxyciphersuite
URL	https://cwe.mitre.org/data/definitions/20.html
URL	http://technet.microsoft.com/security/advisory/2588513
URL	http://support.apple.com/kb/HT4999
URL	http://msdn.microsoft.com/en-us/library/windows/desktop/bb870930(v=vs.85).aspx
URL	http://www.ibm.com/developerworks/java/jdk/alerts/
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02

SSL Connection: Sweet32 Vulnerability — Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

SSL connections which support DES, Triple DES and Blowfish CBC mode cipher suites with block sizes of 64 bits are vulnerable to a Birthday Attack when an attacker is able to capture a long duration session. This is known as the "Sweet32" attack.

Impact:
An attacker who is able to capture an encrypted session which is using the vulnerable CBC mode cipher suites that runs long enough to generate more than 785 gigabytes of traffic, may be able to perform a block cipher collision and recover sensitive data such as session cookies or passwords, or other encrypted data. The difficulty and amount of captured data required to exploit this vulnerability is expected to decrease as attackers improve on the methods used in the proof of concept for this attack.

Solution Details

To mitigate this issue, ensure that all available cipher suites for a given service use at least 128-bit ciphers or disable DES, Triple DES and Blowfish CBC mode ciphers. If it is not feasible to disable these cipher suites, consider limiting HTTP/1.1 Keep-Alive, SPDY and HTTP/2 when 64-bit block ciphers are used in order to prevent a session from running long enough to be viable for a Sweet32 attack.

CVSS Base Score: 5

CVSS Vector: AV:N/AC:L/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-2183
BUGTRAQ	http://www.securityfocus.com/bid/95568
BUGTRAQ	http://www.securityfocus.com/bid/92630
URL	http://www-01.ibm.com/support/docview.wss?uid=nas8N1021697
URL	http://www.oracle.com/technetwork/security-advisory/cpujan2018-3236628.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html
URL	https://security.netapp.com/advisory/ntap-20160915-0001/
URL	https://security.netapp.com/advisory/ntap-20170119-0001/
URL	https://www.tenable.com/security/tns-2017-09
URL	https://cwe.mitre.org/data/definitions/200.html
URL	https://www.tenable.com/security/tns-2016-21
URL	https://www.tenable.com/security/tns-2016-20
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2017-3236626.html
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbgn03765en_us

Type	Reference
URL	http://www.oracle.com/technetwork/security-advisory/cpujul2017-3236622.html
URL	https://h20566.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03725en_us
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390849
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05385680
URL	https://www.tenable.com/security/tns-2016-16
URL	http://www-01.ibm.com/support/docview.wss?uid=swg21991482
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05369415
URL	https://bto.bluecoat.com/security-advisory/sa133
URL	https://kc.mcafee.com/corporate/index?page=content&id=SB10171
URL	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA40312
URL	https://www.suse.com/security/cve/CVE-2016-2183.html
URL	https://security-tracker.debian.org/tracker/CVE-2016-2183
URL	https://quickview.cloudapps.cisco.com/quickview/bug/CSCvb05575
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05323116
URL	https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05309984
URL	https://community.qualys.com/thread/16555
URL	https://bugzilla.suse.com/show_bug.cgi?id=995359
URL	https://bugs.python.org/issue27850
URL	http://www.securityfocus.com/bid/92630/references

Type	Reference
URL	https://nodejs.org/en/blog/vulnerability/september-2016-security-releases/
URL	http://www.oracle.com/technetwork/topics/security/ovmbulletinoct2016-3090547.html
URL	http://www.oracle.com/technetwork/topics/security/linuxbulletinoct2016-3090545.html
URL	http://www.oracle.com/technetwork/security-advisory/cpuoct2016-2881722.html
URL	https://www.openssl.org/blog/blog/2016/08/24/sweet32/
URL	https://bugzilla.redhat.com/show_bug.cgi?id=1369383
URL	https://access.redhat.com/security/cve/cve-2016-2183
URL	https://access.redhat.com/articles/2548661
URL	https://www.teskalabs.com/blog/teskalabs-bulletin-160826-seacat-sweet32-issue
URL	https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2016/august/new-practical-attacks-on-64-bit-block-ciphers-3des-blowfish/
URL	https://sweet32.info/
URL	https://nakedsecurity.sophos.com/2016/08/25/anatomy-of-a-cryptographic-collision-the-sweet32-attack/
URL	https://github.com/ssllabs/ssllabs-scan/issues/387#issuecomment-242514633
URL	https://blog.cryptographyengineering.com/2016/08/24/attack-of-week-64-bit-ciphers-in-tls/
URL	https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-02
URL	https://www.mitel.com/en-ca/support/security-advisories/mitel-product-security-advisory-17-0008

SSL Connection: TLS Compression Enabled

Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

The remote TLS endpoint supports compression. TLS compression has been demonstrated to leak information by not obfuscating the length of the underlying compressed and unencrypted data.

One attack that exploits this weakness is called "Compression Ratio Info-leak Made Easy" (CRIME). CRIME allows man-in-the-middle attackers to decrypt data by injecting guesses of the content of the plaintext into the encrypted traffic and then observing differences in the length of the resulting encrypted packets.
Impact:
An attacker who is able to achieve a man-in-the-middle position and carry out the CRIME attack will be able to read the content of encrypted traffic. This could potentially divulge sensitive cookies, or session IDs which could then be reused by the attacker to gain access to protected resources.

Solution Details

The attacks against TLS compression can be mitigated server-side by disabling this functionality on the affected server.

Apache versions 2.4.3 and 2.2.24 using mod_ssl support an option which allows the compression functionality to be disabled. This behavior can be achieved by specifying "SSLCompression off" in the httpd.conf file.

Apache using mod_gnutls supports toggling of TLS compression through the GnuTLSPriorities flag. TLS compression can be disabled by specifying "!COMP-DEFLATE".

CVSS Base Score: 2.6

CVSS Vector: AV:N/AC:H/Au:N/C:P/I:N/A:N

Type	Reference
CVE	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4929
BUGTRAQ	http://www.securityfocus.com/bid/55704
URL	https://threatpost.com/en_us/blogs/demo-crime-tls-attack-091212
URL	https://gist.github.com/3696912
URL	http://code.google.com/p/chromium/issues/detail?id=139744
URL	http://isecpartners.com/blog/2012/9/14/details-on-the-crime-attack.html
URL	http://arstechnica.com/security/2012/09/crime-hijacks-https-sessions/
URL	http://www.theregister.co.uk/2012/09/14/crime_tls_attack/
URL	https://cwe.mitre.org/data/definitions/310.html
URL	https://github.com/mpgn/CRIME-poc

Type	Reference
URL	https://bugzilla.redhat.com/show_bug.cgi?id=857051
URL	https://chromiumcodereview.appspot.com/10825183
URL	http://news.ycombinator.com/item?id=4510829
URL	http://security.stackexchange.com/questions/19911/crime-how-to-beat-the-beast-successor
URL	https://community.qualys.com/blogs/securitylabs/2012/09/14/crime-information-leakage-attack-against-ssltls
URL	http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091
URL	http://support.apple.com/kb/HT5784

SSL Connection: Weak Ciphers Enabled

Trivial

Solution Details

Configure the server to reject weak SSL ciphers. All supported SSL cipher suites should be at least 128 bit strength. If SSL was included as a bundled software package, please contact the vendor for remediation details.

Common web server implementations:
Apache v2 - Modify the SSLCipherSuite directive in the httpd.conf or ssl.conf file to not allow the use of weak ciphers and restart the Apache server. Note that this may prevent older web browsers from connecting to the website. For more information on specific SSLCipherSuite directives, please refer the Apache mod_ssl SSLCipherSuite online documentation at
http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite.

Microsoft IIS - Please see Microsoft's official enterprise support blog at
http://blogs.technet.com/b/askds/archive/2011/05/04/speaking-in-ciphers-and-other-enigmatic-tongues.aspx
Note that this may prevent older web browsers from connecting to the website.

For other web servers, please consult the vendor specific documentation for the server type.

Vulnerability Details

The SSL protocol supports a suite of ciphers, or cryptographic algorithms, for transmitting certificates, establishing session keys, performing authentication, etc. Some of these ciphers use keys that are very small and thus cryptographically weak. The full set of available ciphers is not equal to the certificate signature algorithm listed in the SSL certificate.

This host's SSL connection accepts one or more weak ciphers as an acceptable transport mechanism for data. A remote attacker with access to an upstream node can leverage this weakness to perform a

"Man in the Middle" attack against this SSL connection, resulting in loss of confidentiality of the transmitted data.

OpenSSL provides a list of SSL cipher suite names and their OpenSSL equivalents which is linked in the reference list of the vulnerability details.

False Positive Notes

This item is not a false positive. Appropriate remediation is required.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	http://www.openssl.org/docs/apps/ciphers.html
URL	http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslciphersuite.

TDS SQL Database Service

Trivial

Vulnerability Details

This host is running a database service that uses the TDS network protocol. The TDS protocol, which stands for the Tabular Data Stream protocol, is used by the Sybase Adaptive Server Anywhere and Microsoft SQL Server database engines. It is a low level protocol that does not provide password or data encryption, and is vulnerable to standard passive network analysis attacks. An attacker who is able to view network traffic between the client and the server can leverage this to obtain database authentication credentials as well as capture the results of any database queries. Aside from the sensitive information leak, an attacker could parlay obtained authentication credentials to completely compromise this host. The TDS service should never be exposed to the Internet.

Solution Details

Please consider using ODBC or OLEDB as a means of remotely accessing this host's database server. If the TDS protocol is required for performance reasons or because other methods of database access are not feasible, please tunnel the database connections through an encrypted VPN or SSL connection.

In general, do not allow database services to be accessed directly from the Internet, especially via TDS.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

TLS Connection: TLS Version 1.0 Enabled

Trivial

Vulnerability Details

This host appears to support Transport Layer Security version 1.0 (TLSv1.0). The PCI Security Standards Council has declared that TLSv1.0 no longer meets minimum security standards. This is in large part due to vulnerabilities within the TLSv1.0 protocol that cannot be fixed.

Solution Details

Due to its inherent weaknesses, please consider disabling support for TLSv1.0 and only supporting newer protocols such as TLSv1.1 and TLSv1.2. Consult your specific vendor documentation for more information.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://en.wikipedia.org/wiki/Transport_Layer_Security

TLS Connection: TLS Version 1.1 Enabled

Trivial

Solution Details

Due to its inherent weaknesses, please consider disabling support for TLSv1.1 and only supporting newer protocols such as TLSv1.2 and TLSv1.3. Consult your specific vendor documentation for more information.

Vulnerability Details

This host appears to support Transport Layer Security version 1.1 (TLSv1.1). This protocol is out of date and does not support modern cryptographic algorithms and as a result, many browsers no longer support TLS 1.1.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
URL	https://en.wikipedia.org/wiki/Transport_Layer_Security

TLS Connection: TLS Version 1.2 Not Enabled — Trivial

Solution Details

Consider only supporting newer protocols such as TLSv1.2 and TLSv1.3. Consult your specific vendor documentation for more information.

Vulnerability Details

This host appears to not support Transport Layer Security version 1.2 (TLSv1.2). This protocol is necessary to use modern cryptographic algorithms.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Web Server Default Error Page Detected — Trivial

Vulnerability Details

This asset is running a web server service which is configured to use default error responses.
Impact:
A remote attacker may be able to leverage these default error responses to gather information about this asset.

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Solution Details

Refer to the documentation for your web server regarding using custom error pages.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	

Web Server Directory Structure Disclosure — Trivial

False Positive Notes

This item is not likely to be a false positive. Please validate and document remediation efforts through Active View.

Vulnerability Details

This host's web application discloses information that details the directory structure of the underlying host OS. This type of information is typically disclosed in verbose error messages or in file links which utilize fully qualified paths instead of relative paths. Attackers can use this type of information to hone more specific attacks against the web application or the underlying host OS.

Solution Details

Ensure that verbose error messages are disabled and that all references to files within the web application are relative paths.

CVSS Base Score: 0

CVSS Vector: AV:N/AC:L/Au:N/C:N/I:N/A:N

Type	Reference
There are no references for this vulnerability.	