WHITE PAPER

Tripwire Vulnerability Risk Metrics

Connecting Security to the Business

IRFAHN KHIMJI, CISSP

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

A vulnerability management program should provide a series of metrics that outline the vulnerability risk to the organization and how the risk posture is trending. In addition to this, reports should be provided which show system owners which vulnerabilities pose the greatest risk to the organization and how to remediate them. This report outlines recommendations for vulnerability management reporting based off of industry best practices.

Tripwire Vulnerability Management Overview

Tripwire's IT security solutions reduce risk, ensure systems and data security, and automate attainment of regulatory compliance objectives. Tripwire offerings solve the security configuration management, vulnerability management, continuous monitoring and incident detection problems facing organizations of all sizes, as stand-alone solutions or in concert with other IT security controls. Ultimately, Tripwire helps detect issues, protect sensitive data and positively connect these values to business objectives.

Tripwire's mission statement for vulnerability management is to deliver the most complete and accurate coverage for security issues that matter to real enterprise environments. As such, Tripwire provides a tiered architecture to provide scalability and reliability while scanning in production environments including, but not limited to, DMZs and SCADA environments.

Vulnerability Risk Scoring

The risk a vulnerability or set of vulnerabilities poses needs to be objectively calculated to ensure consistency. Vulnerability severity has been calculated in the industry based on the Common Vulnerability Scoring System (CVSS). This scoring system rates vulnerabilities on a bounded range of 1–10. The problem this poses, however, is that in large organizations there are often too many 9s and 10s to remediate within a reasonable time frame. Therefore, additional information is required.

In addition to providing the CVSS scores, Tripwire provides additional information that objectively rates vulnerabilities based on how easy they are exploit, what privilege an attacker would get upon successful remediation, and the age of the vulnerability. Older vulnerabilities pose a higher threat, as they are the ones being more actively exploited in the wild. The Tripwire scoring system plugs these variables into a formula to provide an unbound integer. This allows for easy visibility to the highest risk vulnerabilities, as well as provides an easy way to trend the risk score across the organization over time.

Furthermore, to simplify vulnerability scoring for the business, who are not information security professionals, a simple High/Medium/Low scoring model is required. Therefore, depending on the audience for the vulnerability report, a different scoring system needs to be applied.

Executive Vulnerability Metrics

When working towards the continuous improvement of any process, the first important thing to do is take a baseline set of metrics for the organization. A common mistake made by most organizations is that the first question asked is, "How many vulnerabilities do we have?" or "How many HIGH vulnerabilities do we have?" This metric, while serving a purpose, does not provide a good sense of the overall risk trend of the organization. This metric is typically used when looking at vulnerability risk by CVSS score.

Instead, using the Tripwire risk score the first question we would like to answer is, "What is the overall risk posture of our organization?" This metric provides a starting point for reducing the risk within the organization. While specific numbers are not required at this high level, charting this metric over time allows executives to see whether the risk in the organization is trending higher or if efforts to reduce risk are paying off. Figure 1 shows an example of a Tripwire risk score over time; over the course of the twelve weeks this metric has been tracked the overall risk posture has been relatively steady.

For further details, the same metric can be broken down into the individual management groups within the organization as shown in Figure 2. In this example, the organization is broken down by ownership of the operating system type. However, the groups can be organized based on the needs of each specific organization.

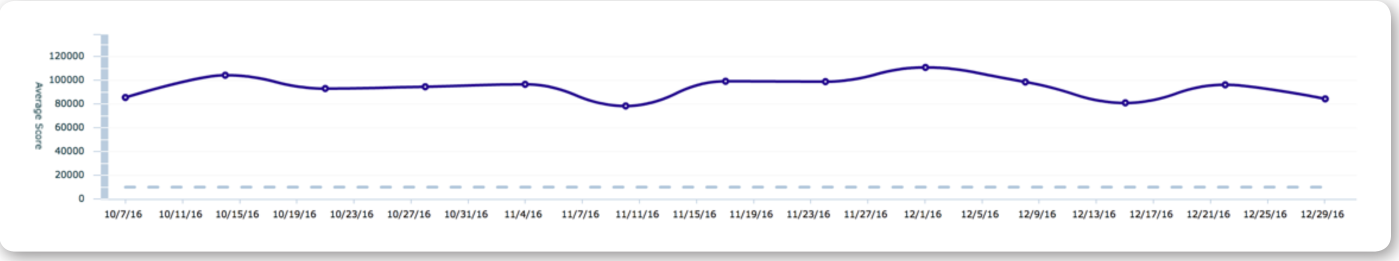


Fig. 1 Example of a Tripwire vulnerability risk score over time

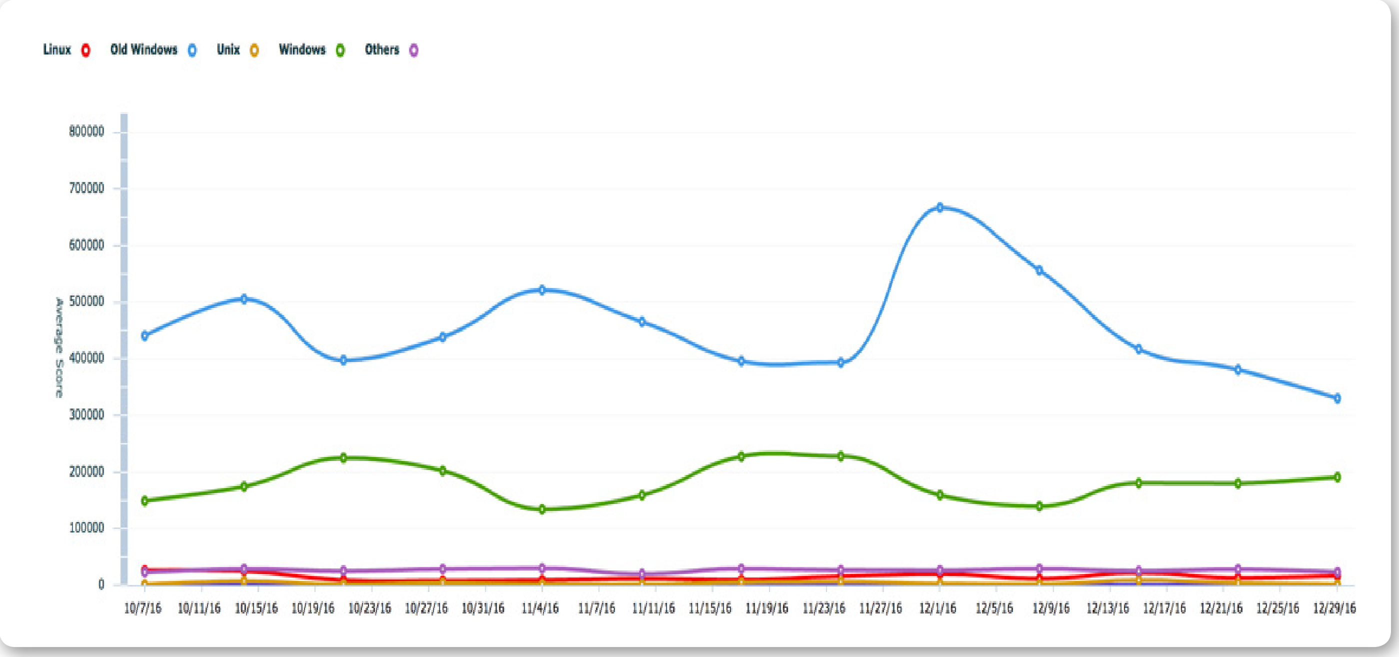


Fig. 2 Overall risk posture of an organization

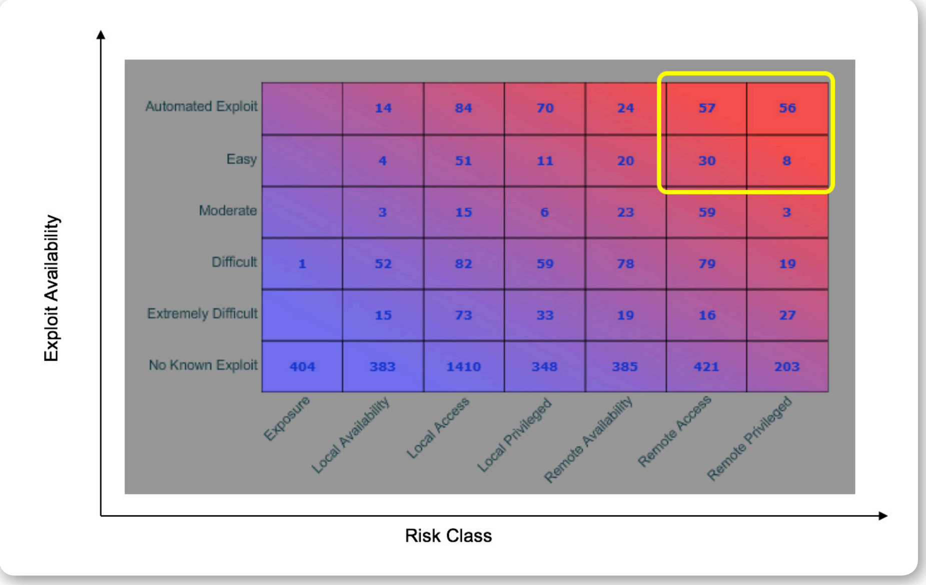
Upon analysis of this graph, we see that the two greatest contributors to the risk of the organization are old Windows operating systems which are no longer supported, as well as our current Windows operating systems. In order to greatly reduce the risk posture of the organization, we can initiate a project to migrate off of the older, unsupported, operating systems.

Furthermore, we see that the vulnerability risk in each of the areas has remained relatively steady. We can set goals to reduce this risk depending on the risk tolerance of the organization, as well as the aggressiveness with which the executives would like to reduce the risk.

Typically, organizations in the early stages of their vulnerability management program have average Tripwire risk scores well over the 20,000 range. In contrast, very mature organizations are able to keep their risk scores below 5000. In order to get to that level of maturity, most organizations will set risk reduction targets between 10% and 20% year-over-year. This allows their teams to focus both on remediating existing risks as well as keeping up to date with current patch levels as new threats emerge.

Now that we have seen how the example organization is trending, let us dive further into the specific metrics that provide a deeper understanding of its current security posture. The first metric (Figure 3) shows a heat map of the criticality of vulnerabilities based on the ease of exploit and privilege an attacker will gain upon successful exploitation of the vulnerability.

The first priority of remediation should be the vulnerabilities in the top-right



	Exposure	Local Availability	Local Access	Local Privileged	Remote Availability	Remote Access	Remote Privileged
Automated Exploit		14	84	70	24	57	56
Easy		4	51	11	20	30	8
Moderate		3	15	6	23	59	3
Difficult	1	52	82	59	78	79	19
Extremely Difficult		15	73	33	19	16	27
No Known Exploit	404	383	1410	348	385	421	203

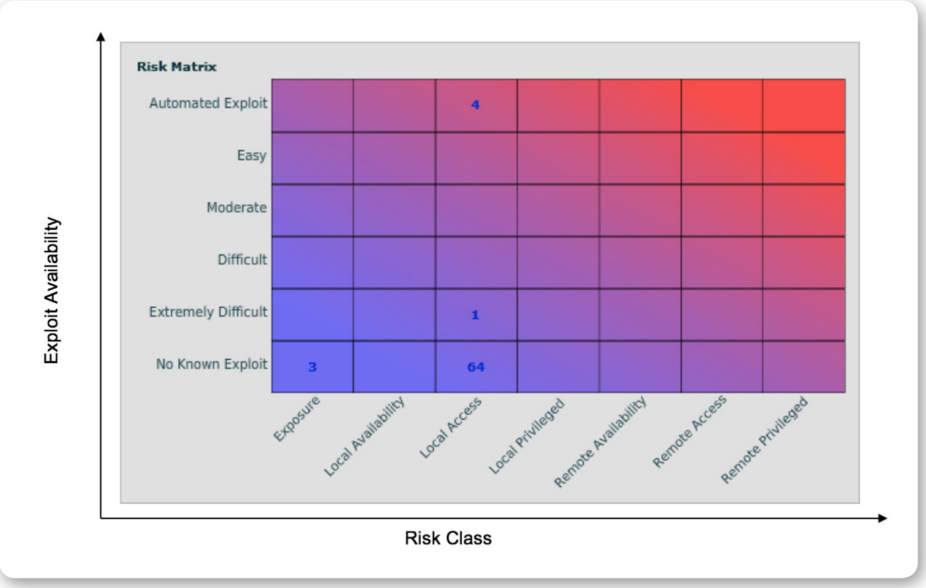
Fig. 3 Heat map of vulnerability criticality

corner of the matrix as those vulnerabilities pose a risk of an attacker being able to remotely exploit the vulnerability with ›minimal effort. These are "low hanging fruit" that should be immediately addressed. Following that, any vulnerability with an automated exploit should be remediated as minimal effort is required for successful exploitation.

Figure 3 shows the vulnerability numbers across an organization, but can easily be filtered to show the same matrix for only vulnerabilities assigned to a particular owner. Similarly, filters can be applied to only show the results for a particular application. A common metric desired by organizations is to know how many vulnerabilities are present in Java and Adobe applications, as seeen in Figure 4.

Teams that are typically overwhelmed by remediating hundreds of vulnerabilities, can focus on the ones that will have the greatest impact to the organization. In this example, they can focus on remediating the four vulnerabilities that have automated exploits associated first, before moving into remediating other vulnerabilities.

Some other key metrics to consider are host, vulnerability, and application metrics. Figure 5 shows some out-of-the-box metrics to consider when evaluating a vulnerability management program.



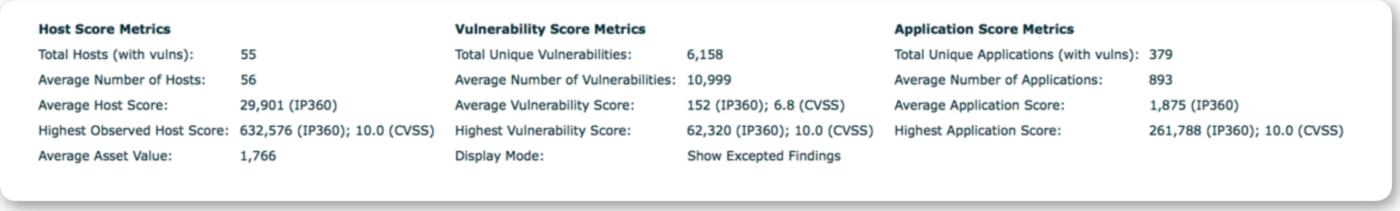
Risk Matrix

	Exposure	Local Availability	Local Access	Local Privileged	Remote Availability	Remote Access	Remote Privileged
Automated Exploit			4				
Easy							
Moderate							
Difficult							
Extremely Difficult			1				
No Known Exploit	3		64				

Fig. 4 Vulnerabilities for Java and Adobe applications

It's also important to identify the trend of hosts and vulnerabilities identified over time. Figure 6 shows the difference between two points in time across the entire organization.

One can see that while there were a high number of vulnerabilities not remediated, there was made progress in remediating 1608 vulnerabilities. These numbers can also be further broken out by department or system owner based on the requirements of each specific organization.

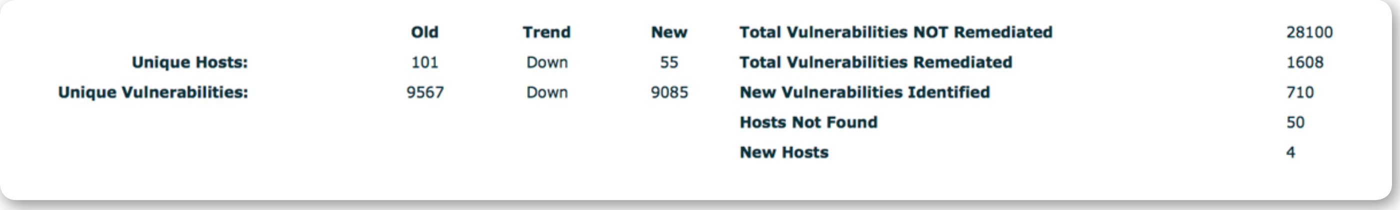


Host Score Metrics	
Total Hosts (with vulns):	55
Average Number of Hosts:	56
Average Host Score:	29,901 (IP360)
Highest Observed Host Score:	632,576 (IP360); 10.0 (CVSS)
Average Asset Value:	1,766

Vulnerability Score Metrics	
Total Unique Vulnerabilities:	6,158
Average Number of Vulnerabilities:	10,999
Average Vulnerability Score:	152 (IP360); 6.8 (CVSS)
Highest Vulnerability Score:	62,320 (IP360); 10.0 (CVSS)
Display Mode:	Show Excepted Findings

Application Score Metrics	
Total Unique Applications (with vulns):	379
Average Number of Applications:	893
Average Application Score:	1,875 (IP360)
Highest Application Score:	261,788 (IP360); 10.0 (CVSS)

Fig. 5 Out-of-the-box metrics to consider when evaluating the vulnerability management program



	Old	**Trend**	**New**
Unique Hosts:	101	Down	55
Unique Vulnerabilities:	9567	Down	9085

Total Vulnerabilities NOT Remediated	28100
Total Vulnerabilities Remediated	1608
New Vulnerabilities Identified	710
Hosts Not Found	50
New Hosts	4

Fig. 6 The difference between two points in time across the entire organization

Operational Vulnerability Reports

An alarming, yet common, trend among organizations is to run a report that contains all of the vulnerabilities found under a particular system owner and send them a very large report. Some organizations have matured beyond that to provide reports that only include everything that is a "High" score. The main question then becomes, what defines a high-scoring vulnerability? To answer this, security analysts have typically said anything that is a CVSS 7 or above should be remediated. The PCI standard, for example, says that a CVSS score of 7.0–10.0 is High, 4.0–6.9 is Medium, and 0.0–3.9 is Low.

In common practice, system administrators have said that there are far too many vulnerabilities that with a CVSS score of 10 and above to remediate within a reasonable amount of time. Depending on the organization, system administrators have committed to remediating anywhere from one to 10 vulnerabilities per month. So the first question they pose to the security analysts is, "which of these vulnerabilities with a CVSS score of 10 is the most severe?"

The Tripwire vulnerability risk score alleviates this problem. Figure 7 illustrates that by providing the specific details of the ease of exploit, the privilege gained, and the age of the vulnerability, security analysts have a simple, objective answer to provide to system administrators. In some cases, based off of these factors, a vulnerability that has a CVSS score below 10 might pose more of a risk to the organization than one with a CVSS score of 10.

In some cases, system administrators will channel their remediation efforts on either a per-host or per-vulnerability basis. If they choose to remediate per-host, Tripwire can provide a report that shows the top 10 most at-risk hosts. See Figure 8 for an example.

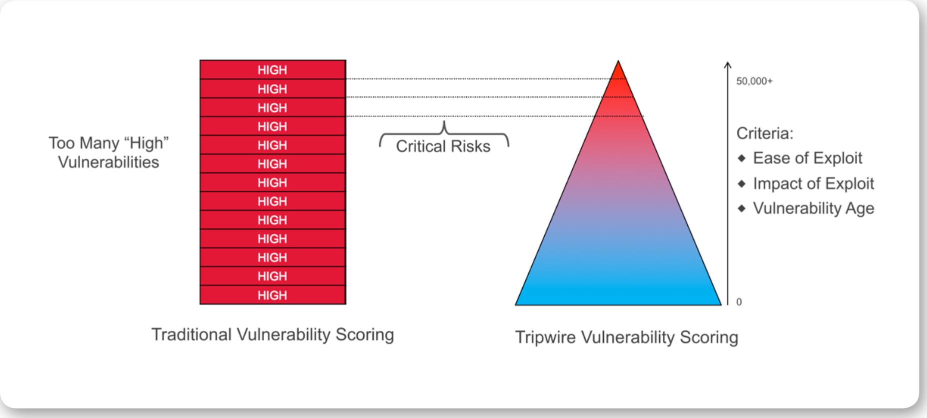
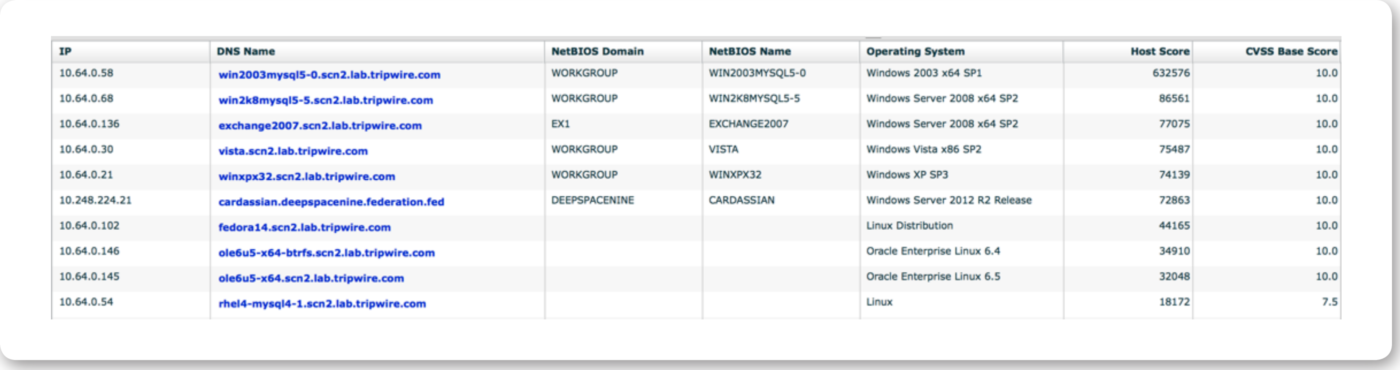
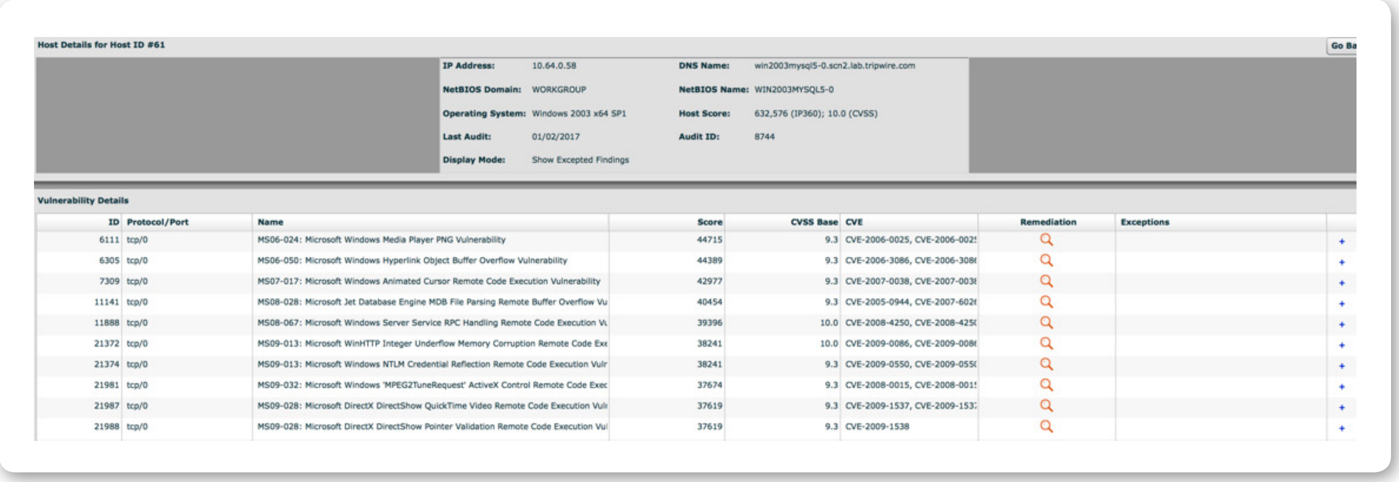


Fig. 7 Tripwire IP360 vulnerability risk score vs. traditional risk scoring



IP	DNS Name	NetBIOS Domain	NetBIOS Name	Operating System	Host Score	CVSS Base Score
10.64.0.58	win2003mysql5-0.scn2.lab.tripwire.com	WORKGROUP	WIN2003MYSQL5-0	Windows 2003 x64 SP1	632576	10.0
10.64.0.68	win2k8mysql5-5.scn2.lab.tripwire.com	WORKGROUP	WIN2K8MYSQL5-5	Windows Server 2008 x64 SP2	86561	10.0
10.64.0.136	exchange2007.scn2.lab.tripwire.com	EX1	EXCHANGE2007	Windows Server 2008 x64 SP2	77075	10.0
10.64.0.30	vista.scn2.lab.tripwire.com	WORKGROUP	VISTA	Windows Vista x86 SP2	75487	10.0
10.64.0.21	winxpx32.scn2.lab.tripwire.com	WORKGROUP	WINXPX32	Windows XP SP3	74139	10.0
10.248.224.21	cardassian.deepspacenine.federation.fed	DEEPSPACENINE	CARDASSIAN	Windows Server 2012 R2 Release	72863	10.0
10.64.0.102	fedora14.scn2.lab.tripwire.com			Linux Distribution	44165	10.0
10.64.0.146	ole6u5-x64-btrfs.scn2.lab.tripwire.com			Oracle Enterprise Linux 6.4	34910	10.0
10.64.0.145	ole6u5-x64.scn2.lab.tripwire.com			Oracle Enterprise Linux 6.5	32048	10.0
10.64.0.54	rhel4-mysql4-1.scn2.lab.tripwire.com			Linux	18172	7.5

Fig. 8 Target per-host report



Host Details for Host ID #61

IP Address:	10.64.0.58	**DNS Name:**	win2003mysql5-0.scn2.lab.tripwire.com
NetBIOS Domain:	WORKGROUP	**NetBIOS Name:**	WIN2003MYSQL5-0
Operating System:	Windows 2003 x64 SP1	**Host Score:**	632,576 (IP360); 10.0 (CVSS)
Last Audit:	01/02/2017	**Audit ID:**	8744
Display Mode:	Show Excepted Findings		

Vulnerability Details

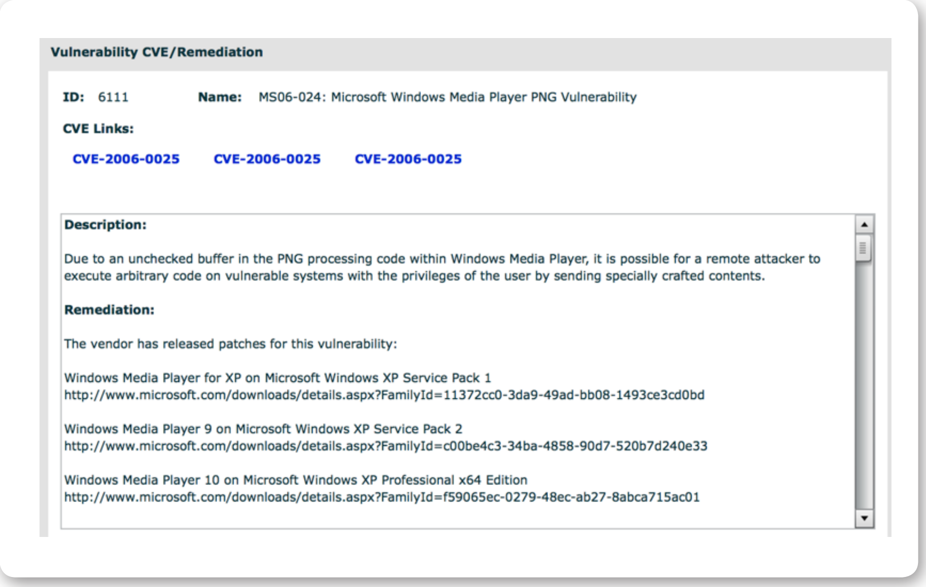
ID	Protocol/Port	Name	Score	CVSS Base	CVE	Remediation	Exceptions	
6111	tcp/0	MS06-024: Microsoft Windows Media Player PNG Vulnerability	44715	9.3	CVE-2006-0025, CVE-2006-002	🔍		+
6305	tcp/0	MS06-050: Microsoft Windows Hyperlink Object Buffer Overflow Vulnerability	44389	9.3	CVE-2006-3086, CVE-2006-308	🔍		+
7309	tcp/0	MS07-017: Microsoft Windows Animated Cursor Remote Code Execution Vulnerability	42977	9.3	CVE-2007-0038, CVE-2007-003	🔍		+
11141	tcp/0	MS08-028: Microsoft Jet Database Engine MDB File Parsing Remote Buffer Overflow Vu	40454	9.3	CVE-2005-0944, CVE-2007-602	🔍		+
11888	tcp/0	MS08-067: Microsoft Windows Server Service RPC Handling Remote Code Execution Vu	39396	10.0	CVE-2008-4250, CVE-2008-425	🔍		+
21372	tcp/0	MS09-013: Microsoft WinHTTP Integer Underflow Memory Corruption Remote Code Exe	38241	10.0	CVE-2009-0086, CVE-2009-008	🔍		+
21374	tcp/0	MS09-013: Microsoft Windows NTLM Credential Reflection Remote Code Execution Vulr	38241	9.3	CVE-2009-0550, CVE-2009-055	🔍		+
21981	tcp/0	MS09-032: Microsoft Windows 'MPEG2TuneRequest' ActiveX Control Remote Code Exec	37674	9.3	CVE-2008-0015, CVE-2008-001	🔍		+
21987	tcp/0	MS09-028: Microsoft DirectX DirectShow QuickTime Video Remote Code Execution Vulr	37619	9.3	CVE-2009-1537, CVE-2009-153	🔍		+
21988	tcp/0	MS09-028: Microsoft DirectX DirectShow Pointer Validation Remote Code Execution Vul	37619	9.3	CVE-2009-1538	🔍		+

Fig. 9 The top 10 vulnerabilities within the highest scoring host from the report in Fig 8

Each one of these hosts can then be investigated further to show the top vulnerabilities, along with their remediation details. Figure 9 is an example of the top 10 vulnerabilities within the highest scoring host from the report example in Figure 8. Figure 10 shows a subset of the remediation information of the highest risk vulnerability within that report.

If the system administrators prefers to channel their remediation efforts on a per-vulnerability basis, we can look at the reports based on the vulnerability risk score to see the 10 most severe vulnerabilities within the organization, as seen in Figure 11.

One of the most common frustrations for information security analysts is false positives in the data. When the data collected can't be trusted, the system administrators lose confidence in both the analyst and the solution providing the data. While no solution is perfect, Tripwire strives to be as accurate as possible, with a <1% false positive rate.



Vulnerability CVE/Remediation

ID: 6111 **Name:** MS06-024: Microsoft Windows Media Player PNG Vulnerability

CVE Links:

CVE-2006-0025 CVE-2006-0025 CVE-2006-0025

Description:

Due to an unchecked buffer in the PNG processing code within Windows Media Player, it is possible for a remote attacker to execute arbitrary code on vulnerable systems with the privileges of the user by sending specially crafted contents.

Remediation:

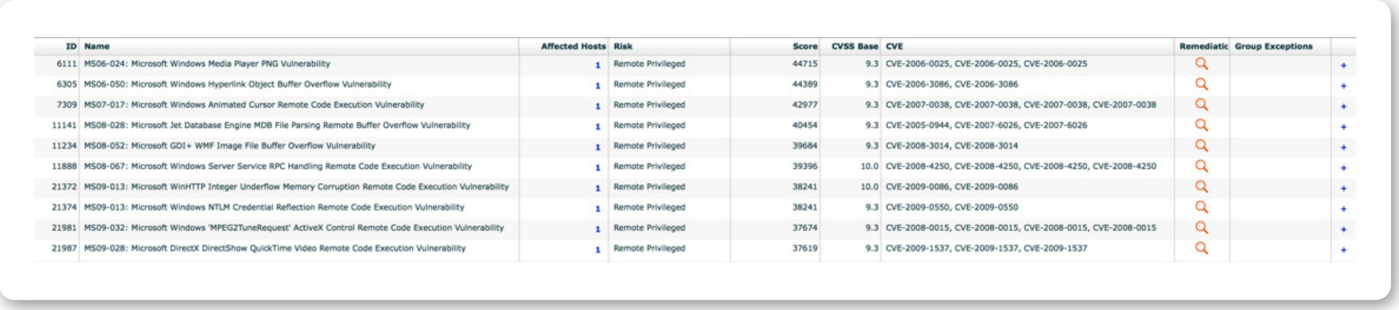
The vendor has released patches for this vulnerability:

Windows Media Player for XP on Microsoft Windows XP Service Pack 1
http://www.microsoft.com/downloads/details.aspx?FamilyId=11372cc0-3da9-49ad-bb08-1493ce3cd0bd

Windows Media Player 9 on Microsoft Windows XP Service Pack 2
http://www.microsoft.com/downloads/details.aspx?FamilyId=c00be4c3-34ba-4858-90d7-520b7d240e33

Windows Media Player 10 on Microsoft Windows XP Professional x64 Edition
http://www.microsoft.com/downloads/details.aspx?FamilyId=f59065ec-0279-48ec-ab27-8abca715ac01

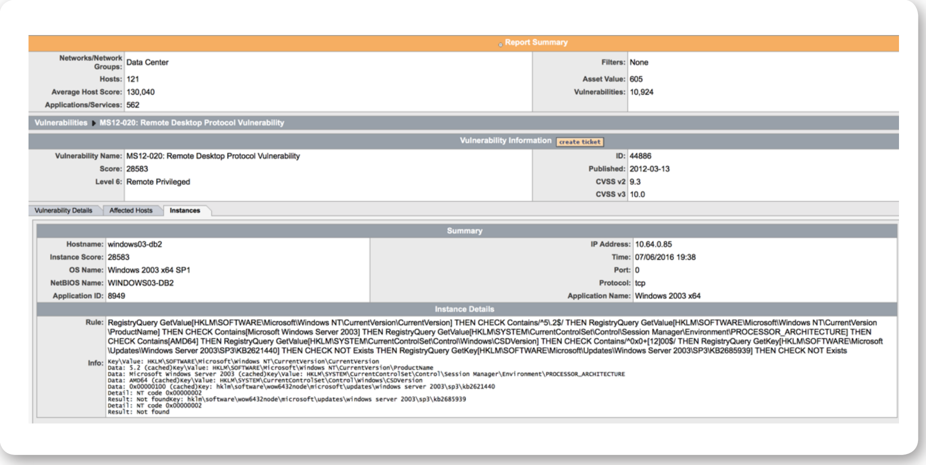
Fig. 10 A subset of the remediation information of the highest risk vulnerabilities found in the report from Fig. 9



ID	Name	Affected Hosts	Risk	Score	CVSS Base	CVE	Remediatic	Group Exceptions	
6111	MS06-024: Microsoft Windows Media Player PNG Vulnerability	1	Remote Privileged	44715	9.3	CVE-2006-0025, CVE-2006-0025, CVE-2006-0025	🔍		+
6305	MS06-050: Microsoft Windows Hyperlink Object Buffer Overflow Vulnerability	1	Remote Privileged	44389	9.3	CVE-2006-3086, CVE-2006-3086	🔍		+
7309	MS07-017: Microsoft Windows Animated Cursor Remote Code Execution Vulnerability	1	Remote Privileged	42977	9.3	CVE-2007-0038, CVE-2007-0038, CVE-2007-0038, CVE-2007-0038	🔍		+
11141	MS08-028: Microsoft Jet Database Engine MDB File Parsing Remote Buffer Overflow Vulnerability	1	Remote Privileged	40454	9.3	CVE-2005-0944, CVE-2007-6026, CVE-2007-6026	🔍		+
11234	MS08-052: Microsoft GDI+ WMF Image File Buffer Overflow Vulnerability	1	Remote Privileged	39684	9.3	CVE-2008-3014, CVE-2008-3014	🔍		+
11888	MS08-067: Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability	1	Remote Privileged	39396	10.0	CVE-2008-4250, CVE-2008-4250, CVE-2008-4250, CVE-2008-4250	🔍		+
21372	MS09-013: Microsoft WinHTTP Integer Underflow Memory Corruption Remote Code Execution Vulnerability	1	Remote Privileged	38241	10.0	CVE-2009-0086, CVE-2009-0086	🔍		+
21374	MS09-013: Microsoft Windows NTLM Credential Reflection Remote Code Execution Vulnerability	1	Remote Privileged	38241	9.3	CVE-2009-0550, CVE-2009-0550	🔍		+
21981	MS09-032: Microsoft Windows 'MPEG2TuneRequest' ActiveX Control Remote Code Execution Vulnerability	1	Remote Privileged	37674	9.3	CVE-2008-0015, CVE-2008-0015, CVE-2008-0015, CVE-2008-0015	🔍		+
21987	MS09-028: Microsoft DirectX DirectShow QuickTime Video Remote Code Execution Vulnerability	1	Remote Privileged	37619	9.3	CVE-2009-1537, CVE-2009-1537, CVE-2009-1537	🔍		+

Fig. 11 Reports based on the vulnerability risk score

For each vulnerability detected, Tripwire provides detection evidence. In many cases, just because a patch is applied it does not necessarily mean that the vulnerability is remediated. In these cases, sometimes a reboot is required or a vulnerable file needs to be manually removed for complete remediation. Figure 12 is an example of the detection evidence that Tripwire provides for each vulnerability.



Report Summary

Networks/Network Groups:	Data Center	Filters:	None
Hosts:	121	Asset Value:	605
Average Host Score:	130,040	Vulnerabilities:	10,924
Applications/Services:	562		

Vulnerabilities ▸ MS12-020: Remote Desktop Protocol Vulnerability

Vulnerability Information create ticket

Vulnerability Name:	MS12-020: Remote Desktop Protocol Vulnerability	ID:	44886
Score:	28583	Published:	2012-03-13
Level 6:	Remote Privileged	CVSS v2	9.3
		CVSS v3	10.0

Summary

Hostname:	windows03-db2	IP Address:	10.64.0.85
Instance Score:	28583	Time:	07/06/2016 19:38
OS Name:	Windows 2003 x64 SP1	Port:	0
NetBIOS Name:	WINDOWS03-DB2	Protocol:	tcp
Application ID:	8949	Application Name:	Windows 2003 x64

Instance Details

Rule: RegistryQuery GetValue[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CurrentVersion] THEN CHECK Contains/^5\.2$/ THEN RegistryQuery GetValue[HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName] THEN CHECK Contains[Microsoft Windows Server 2003] THEN RegistryQuery GetValue[HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\PROCESSOR_ARCHITECTURE] THEN CHECK Contains[AMD64] THEN RegistryQuery GetValue[HKLM\SYSTEM\CurrentControlSet\Control\Windows\CSDVersion] THEN CHECK Contains/^0x0+[12]00$/ THEN RegistryQuery GetKey[HKLM\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB2621440] THEN CHECK NOT Exists THEN RegistryQuery GetKey[HKLM\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP3\KB2685939] THEN CHECK NOT Exists

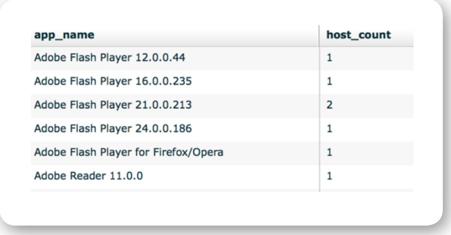
Info:
```
Key\Value: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\CurrentVersion
Data: 5.2 (cached)Key\Value: HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProductName
Data: Microsoft Windows Server 2003 (cached)Key\Value: HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment\PROCESSOR_ARCHITECTURE
Data: AMD64 (cached)Key\Value: HKLM\SYSTEM\CurrentControlSet\Control\Windows\CSDVersion
Data: 0x00000100 (cached)Key: hklm\software\wow6432node\microsoft\updates\windows server 2003\sp3\kb2621440
Detail: NT code 0x00000002
Result: Not foundKey: hklm\software\wow6432node\microsoft\updates\windows server 2003\sp3\kb2685939
Detail: NT code 0x00000002
Result: Not found
```

Fig. 12 Report that provides the detection evidence Tripwire IP360 provides for each vulnerability

Zero-Days and Application Licensing

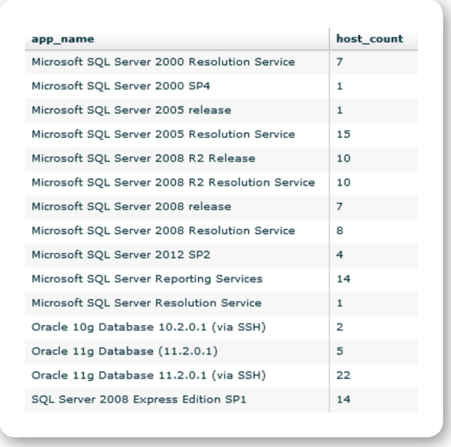
There are many cases where a zero-day vulnerability is announced and specific vulnerability detection coverage is not available. In these cases, information is provided to show which version(s) of the application(s) are affected. Using Tripwire reporting, a new scan doesn't necessarily need to be run to identify which systems are vulnerable. A simple report can be run to show how many of each version of the application is running using the most recent scan data. Figure 13 is report example that shows how many hosts are running which versions of Adobe applications.

Similarly, this data can be used to determine software license counts for applications (such as database instances) across the organization, as shown in Figure 14.



app_name	host_count
Adobe Flash Player 12.0.0.44	1
Adobe Flash Player 16.0.0.235	1
Adobe Flash Player 21.0.0.213	2
Adobe Flash Player 24.0.0.186	1
Adobe Flash Player for Firefox/Opera	1
Adobe Reader 11.0.0	1

Fig. 13 Report showing how many hosts are running which versions of Adobe application



app_name	host_count
Microsoft SQL Server 2000 Resolution Service	7
Microsoft SQL Server 2000 SP4	1
Microsoft SQL Server 2005 release	1
Microsoft SQL Server 2005 Resolution Service	15
Microsoft SQL Server 2008 R2 Release	10
Microsoft SQL Server 2008 R2 Resolution Service	10
Microsoft SQL Server 2008 release	7
Microsoft SQL Server 2008 Resolution Service	8
Microsoft SQL Server 2012 SP2	4
Microsoft SQL Server Reporting Services	14
Microsoft SQL Server Resolution Service	1
Oracle 10g Database 10.2.0.1 (via SSH)	2
Oracle 11g Database (11.2.0.1)	5
Oracle 11g Database 11.2.0.1 (via SSH)	22
SQL Server 2008 Express Edition SP1	14

Fig. 14 Report showing software license counts for applications

Conclusion

Vulnerability and risk management is an ongoing process. The most successful programs continuously adapt and are aligned with the risk reduction goals of the cybersecurity program within the organization. The process should be reviewed on a regular basis, and staff should be kept up to date with the latest threats and trends in information security. Ensuring that continuous development is in place for the people, process, and technology will ensure the success of the enterprise vulnerability and risk management program.

In the initial stages of building the program it's not uncommon for an organization to have a very high average vulnerability score and lengthy remediation cycles. The key is to show progress month by month, quarter by quarter, and year by year. The vulnerability risk scores and time to remediation should decrease as teams become more familiar with the process and become more educated on the risks that the attackers pose.

Tripwire is the trusted leader for establishing a strong cybersecurity foundation. Partnering with Fortune 500 enterprises, industrial organizations and government agencies, Tripwire protects the integrity of mission-critical systems spanning physical, virtual, cloud and DevOps environments. Tripwire's award-winning portfolio delivers top critical security controls, including asset discovery, secure configuration management, vulnerability management and log management. As the pioneers of file integrity monitoring (FIM), Tripwire's expertise is built on a 20+ year history of innovation helping organizations discover, minimize and monitor their attack surfaces. **Learn more at tripwire.com**

***The State of Security*: News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook