tripwire

WHITE PAPER

High-impact Vulnerabilities: Are You Prepared?

The question is when—not if—you will be breached

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

In information security, we often hear the phrase "it's not a matter of if, but when" an organization will be hit by a breach. It is now an accepted fact that preventative controls will eventually fail to keep attackers out. This paper offers insight and guidelines on how to prepare for high-impact, unscheduled vulnerabilities.

In this paper, we will highlight how the tactics and strategies to respond to high-impact vulnerabilities differ from those used in other security events, outline the steps organizations can take to prepare for these vulnerabilities before they hit, and provide insight into incident response strategies.

A New Class of Vulnerabilities

Heartbleed

When it hit in April 2014, Heartbleed (CVE-2014-0160) took IT organizations around the world by surprise. Millions of exposed Internet systems were vulnerable to an active exploit that was silent—it left no traces in logs or other evidence until IDS signatures were made available several weeks later. To make matters worse, the very tests used to identify if a system was vulnerable used the same mechanisms as the exploit itself. This made it difficult for security teams to differentiate between probes and active attacks when they finally did have IDS signatures in place to detect exploit attempts.

For a period lasting several weeks, the Internet was caught with its pants down as IT and security teams scrambled to identify and patch vulnerable systems affected by Heartbleed. One challenge many organizations faced was that OpenSSL existed not just within traditional operating systems, but also within network devices and appliances throughout their networks. Many organizations did not have the tools and procedures in place to identify and remediate the vulnerabilities on these devices.

Other SSL Vulnerabilities

Shortly after Heartbleed, more of what have now been termed "high-impact vulnerabilities" were discovered in OpenSSL, as well as other packages and libraries (such as the Bash Shellshock, CVE-2014-6271). The accepted definition of high-impact vulnerabilities are those that have a wide distribution and a high risk of exploitation.

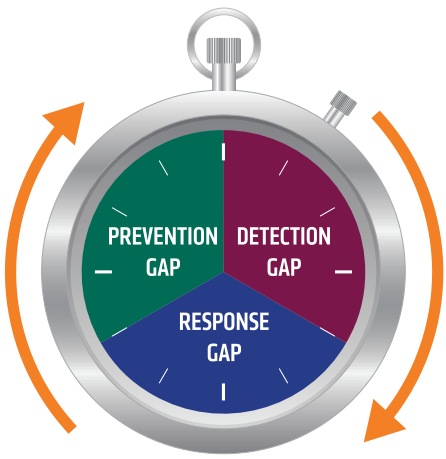
It is expected that more of these vulnerabilities will be discovered as researchers and developers analyze and scrutinize code that was written decades ago. Much of this code has been widely distributed and embedded, not just in traditional servers, but also in a variety of network and security devices and appliances.

Difference Between Predictive and Forecasted Preparation

We can expect to see more high-impact vulnerabilities going forward, so organizations need to prepare themselves for this new normal. Most IT organizations have a vulnerability management and patch cycle in place, but it is usually a regularly scheduled event each month. Let's call this traditional approach a "predictive" model. High-impact vulnerabilities require a different strategy because they are unscheduled and will hit with an increasing, but unpredictable schedule; let's call this approach a "forecasting model."

Preparation and Prevention: The Detection Gap

Identifying and remediating is only the first step in responding to a high-impact vulnerability security incident. If we look at the breach-to-detection gap as coined by Gartner, we can apply this principle within the context of high-impact vulnerabilities. In other words, between when we can assume a system was vulnerable, there is a time gap where that system has likely been exploited, especially if we are able to detect an active exploit hitting the system.



The Detection Gap
The amount of time it takes to discover a compromise and identify its nature. Reports show this often takes five to 18 months.

The Response Gap
The amount of time it takes to identify the full scope of the breach and limit its damage. Research indicates this typically takes over four months.

The Prevention Gap
The time it takes to implement measures to avoid a repeat (or similar) attack.

Fig. 1 The time between breach, discovery and full remediation is a model we call the Enterprise Cyberthreat Gap, to illustrate the different phases of this challenge.

The CIS Controls

Efficacy Of These Controls in Building a Solid Foundation Necessary for Prevention and Quick Response

Throughout this document, we will be referring to the Center for Internet Security's CIS Controls (formerly the Council on CyberSecurity's and SANS 20 Critical Security Controls), with a specific focus on four of the first five controls.

We will demonstrate how these controls apply specifically to a forecasting model of high-impact vulnerability incident pre ention, detection and remediation.

Controls 1 & 2: Take Inventory and Identify Risks

Prevention and Quick Identification of Vulnerable Systems

The CIS Controls provides an excellent executive summary of core security controls every organization should have in place. When it comes to preparing for high-impact vulnerabilities, Controls 1 and 2 should be considered mandatory for mitigating the potential risks associated with these types of threats. Control 1 deals with discovery and inventory of hardware on your network, Control 2 deals with taking an inventory of the software on those assets.

Control 1: Inventory and Control of Hardware Assets

Actively manage (inventory, track and correct) all hardware devices on the network so that only authorized devices are given access to network services and data, and unauthorized and unmanaged devices are found and prevented from gaining access to network assets and data.

Control 2: Inventory and Control of Software Assets

Actively manage (inventory, track and manage) all software on the network so that only authorized software is installed and allowed to execute, and unauthorized and unmanaged software is found and prevented from installation or execution.

Tripwire® IP360™ provides automated discovery and vulnerability management to help IT organizations quickly assess risk and help identify and remediate high-impact vulnerabilities. Tripwire IP360's discovery provides a comprehensive view of your network, supplying a comprehensive inventory of every hardware device and software application. Through Tripwire IP360's integration with Tripwire Enterprise, additional business context can be applied via the tagging of assets, allowing your team to identify critical assets (such as Internet-facing web servers, database servers housing sensitive data, or lower profile assets network devices that are often overlooked) that are affected by high-impact vulnerabilities.

Heartbleed Example

When Heartbleed hit, many organizations were caught off guard because they could not easily identify what systems were affected. Since OpenSSL is integrated into a wide number of software packages, and the list of potentially vulnerable internal assets consists partly of mission-critical internal applications and SSL-enabled services, discovering vulnerable assets could be challenging. These applications include File Transfer Protocol (FTP), Internet Message Access Protocol (IMAP), Post Office Protocol version 3 (POP3), Extensible Messaging and Presence Protocol (XMPP) and Simple Mail Transfer Protocol (SMTP). In addition, many applications depend on OpenSSL packages, making patching production systems a potentially perilous activity if the patch is not fully tested in a lab. Figure 3 shows an example of services that depend on OpenSSL in a typical Linux distribution.

Patching as First Remediation: Heartbleed and Shellshock

When a high-impact vulnerability hits, identification of vulnerable assets and patching status is only the first step in containing the incident within your environment. If you have identified certain systems as being vulnerable, odds are attackers have, too (particularly if those systems are Internet-facing) and they may have already been exploited.

Both Heartbleed and Shellshock had easy to use, remotely executed exploits available almost immediately after the vulnerabilities were discovered. Quickly identifying the window of time a system was vulnerable and analyzing logs from that device and other systems (such as firewalls, IDS and web proxies) for indicators of compromise was crucial, but in these cases tests for vulnerabilities leveraged the same mechanics as active exploit.

Unlike Heartbleed, when Shellshock hit there were forensic artifacts present in log files—the trick was finding them. Tripwire provided custom content for Tripwire Log Center™ to quickly identify those artifacts both through real-time correlation and retroactive analysis via Tripwire Log Center's Audit Logger.

Continuous Vulnerability Assessment and Remediation

Control 3: Continuous Vulnerability Management

Continuously acquire, assess and take action on new information in order to identify and remediate vulnerabilities thereby minimizing the window of opportunity for attackers.

The key word here is "continuously"—instead of just doing a routine vulnerability scan to identify systems that may have high-impact vulnerabilities, we want to continuously monitor the entire network for them. As new devices are added to the network, new applications are installed and operating systems are patched, there is a risk that high-impact and other

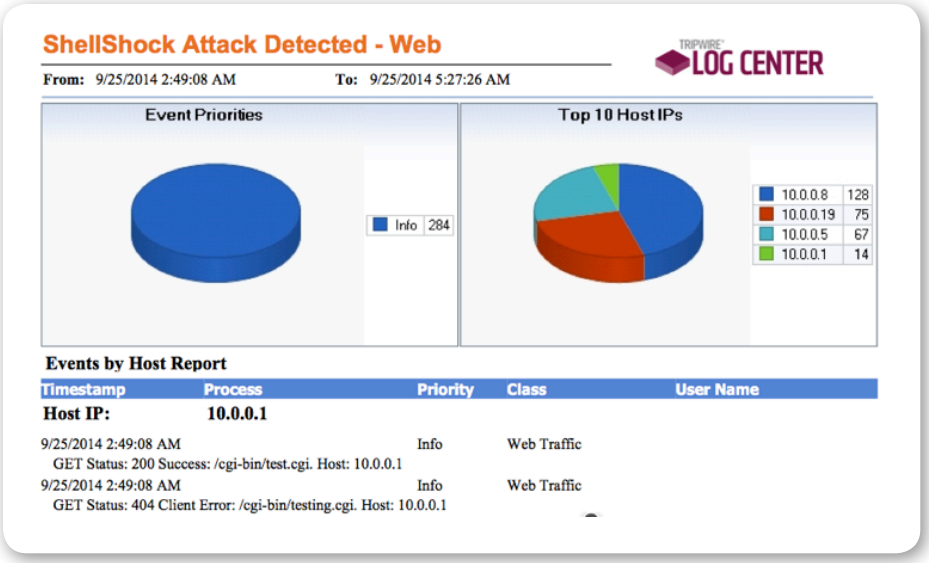


Fig. 2 Shellshock attack detected — Web.

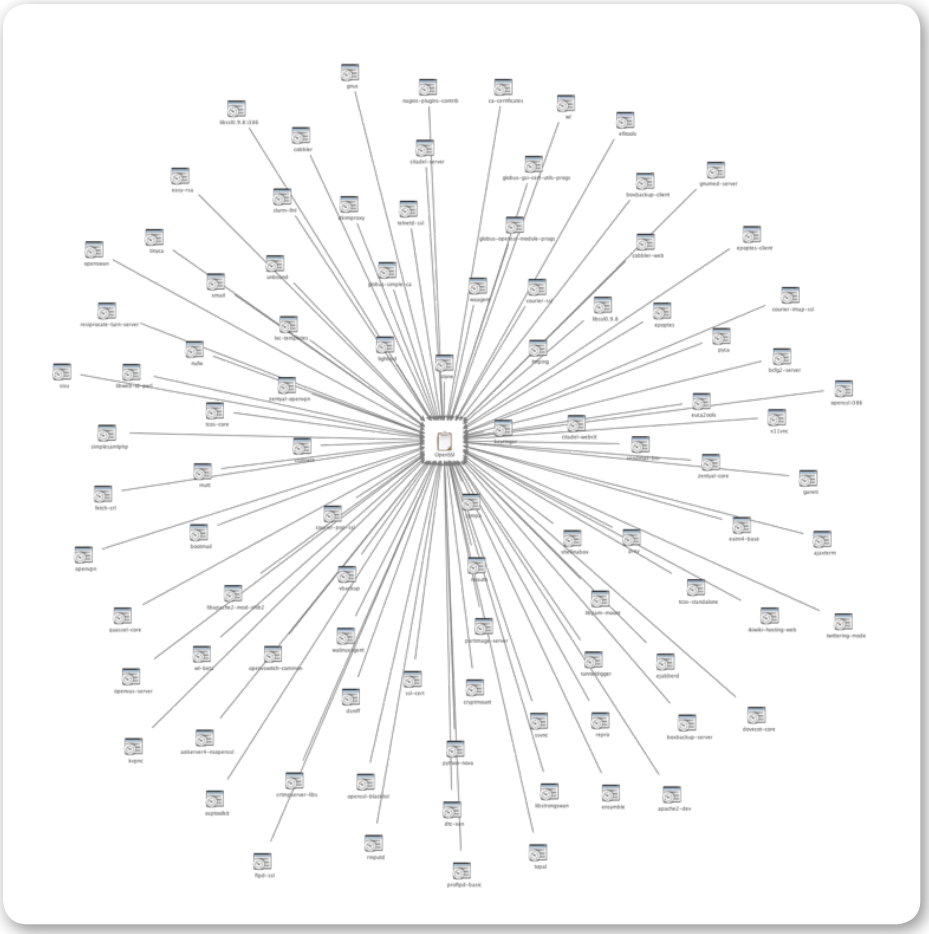


Fig. 3 Example of services linked to OpenSSL on a typical Linux distribution (Ubuntu).

vulnerabilities can be reintroduced to our environments. It's critical to scan beyond traditional servers; all network and security appliances should be continuously monitored. It's also important to have a plan in place to update firmware as it is made available by the manufacturers.

Secure Configuration Hardening: Preparing for Prevention to Fail

Once an attacker gains a foothold into the vulnerable system, they can pivot and move laterally through the network. The high-impact vulnerability scenario has proven to us that, no matter how many resources are allocated to preventive security controls, eventually they will fail. In many respects, the eventual failure of these controls is not within the realm of our control. However, we can prepare for this scenario by ensuring that systems inside our network are properly configured and hardened to make it more difficult on the attacker to expand their attack beyond the initial compromised system. Control 5 highlights this point.

Control 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

Establish, implement and actively manage (track, report on, correct) the security configuration of laptops, servers and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

The CIS Controls provide a great starting point for organizations to communicate security risk to executives; however, when it comes to actual implementation, your organization may want to reference a more granular catalog of controls such as the NIST 800-53 (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf). The following table provides an example of NIST 800-53

controls that are mapped to Control 5 that deal specifically with security configuration management. This provides you an idea of the items organizations should consider in their security configuration management program.

Tripwire has a long history of assisting organizations with the development and maintenance of a secure configuration management program. Tripwire Enterprise delivers change audit and threat detection with exacting precision, as well as intelligent business context and remediation insight. Using Tripwire Enterprise, organizations can deploy a wide range of system configuration policies out-of-the-box that support both security and compliance goals, including NIST 800-53 and CIS benchmarks. These policies can be deployed to ensure systems are configured securely and to detect configuration drift, as well as identify anomalous behavior and other indicators of compromise related to high-impact vulnerabilities and other security threats.

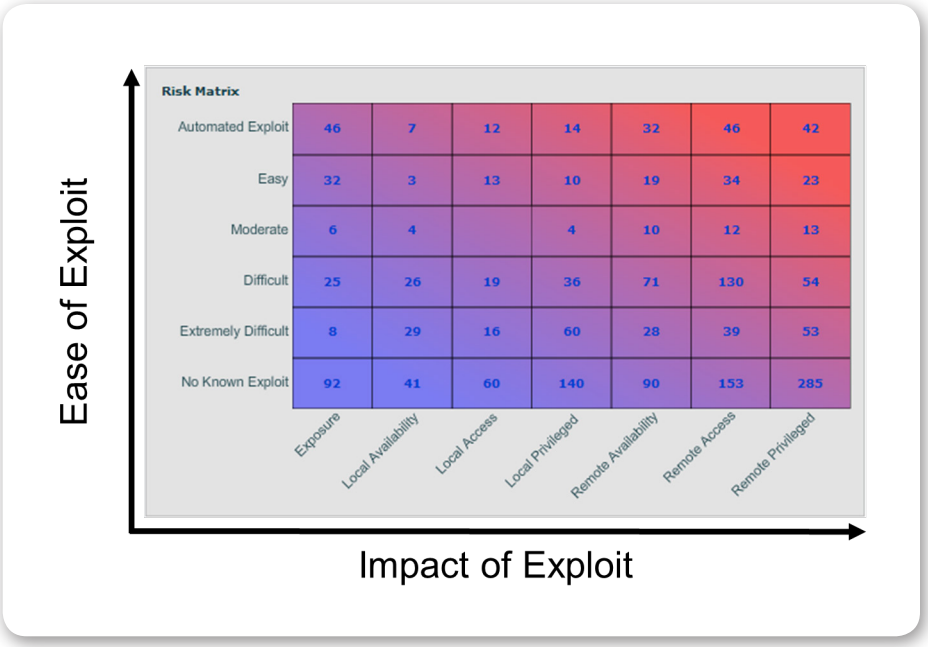


Fig. 4 Tripwire's Vulnerability Risk Matrix is an interactive report that categorizes vulnerabilities based on the ease and impact of exploits, and allows you to drill down into an element to see affected hosts and remediation guidance. The Risk Matrix report is available as an add-on to Tripwire IP360 as a part of the Tripwire Security Intelligence Hub (SIH) reporting and analytics platform.

High-Impact Vulnerability Incident Response Plans Using the Forecasting Model

Preparation and Prevention

Reviewing our typical, predictive incident response flow, we can see how asset discovery helps us better prepare for an incident. An accurate inventory of devices and the software running on them, including the business context of these assets and the data of the assets and data that resides on them, makes it possible to quickly identify vulnerable systems and to detect indicators of compromise.

Detection and Analysis

During the response to a high-impact vulnerability incident, it is critical that the organization first identify which systems were exposed and how long this exposure lasted. Once a catalog of assets has been identified, they should be ranked based on criticality of the asset. Factors to consider include the importance of the asset to business continuity, or whether the asset houses sensitive data.

It's important to audit each critical asset for any security events, as well as any changes made to them. It's also important to ensure that all logins, configuration changes, installed applications and processes running are authorized. It's a good idea to change any passwords on these systems and, depending on the type of vulnerability and level of exposure, revoke and reissue any keys on these systems as well.

Tripwire IP360 can identify the window of time specific systems on a network were vulnerable. However, during the detection and analysis phase, we also need to audit these devices to identify if the systems have been exploited and if there have been any unauthorized changes made to the systems.

By integrating Tripwire IP360 with Tripwire Log Center or other log intelligence tools (such as Splunk), you can analyze log files from the vulnerable system itself as well as from other

NIST 800-53 Control	
CA-07	Continuous Monitoring
CM-02	Baseline Configuration
CM-03	Configuration Change Control
CM-05	Access Restrictions for Change
CM-06	Configuration Settings
CM-07	Least Functionality
CM-08	Information System Component Inventory
CM-09	Configuration Management Plan
CM-11	User-Installed Software
MA-04	Nonlocal Maintenance
RA-05	Vulnerability Scanning
SA-04	Acquisition Process
SC-15	Collaborative Computing Devices
SC-34	Non-Modifiable Executable Programs
SI-02	Flaw Remediation
SI-04	Information System Monitoring

sensors on your network, including firewalls, IDS/IPS and network security monitoring tools such as Bro.

If you currently have a third-party SIEM or log intelligence tool in place, Tripwire Log Center can ingest and normalize log data provided by these tools, and then run correlation rules to identity vulnerabilities. If you don't have a SIEM or log intelligence tool, Tripwire Log Center can independently ingest and normalize your data and run correlation rules out of the box. To get started, a free community edition of Tripwire Log Center is available to Tripwire IP360 and Tripwire Enterprise customers.

Containment and Remediation

In addition to identifying potential exploits and security events on the devices at the network level, we also need to interrogate any vulnerable host to audit all changes made on the device. If the system has been exploited and malware or additional tools were installed, we can use Tripwire Enterprise to identify the installation of any new binaries or configuration changes. The next step is to compare the current state of any potentially compromised host to its last known, trusted state.

In addition to providing identification of any changes, Tripwire Enterprise can also assist with the process of remediating vulnerable and exploited hosts so they can be quickly returned to a trusted state. The combination of Tripwire Enterprise and Tripwire IP360 provides IT organizations with powerful solutions that aid in the remediation process, through detailed guidance as well as monitoring of progress and management of workflow.

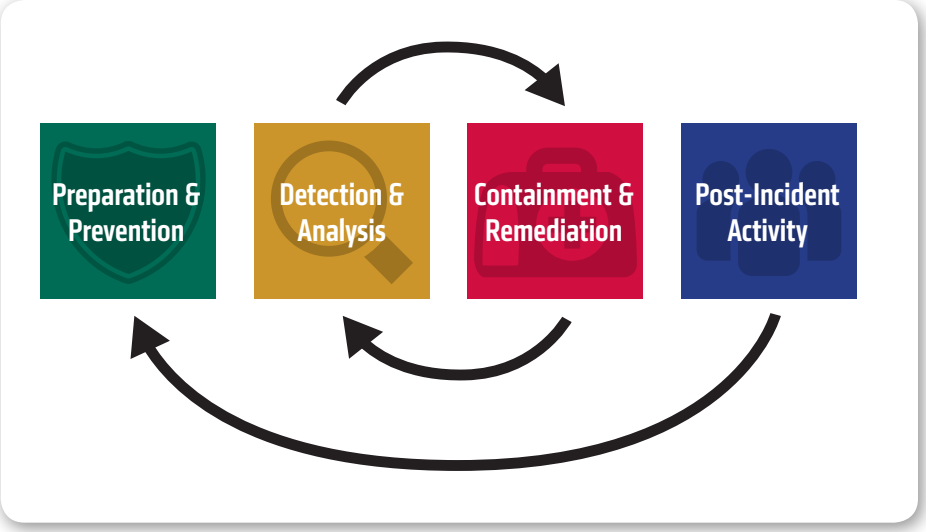


Fig. 5 Diagram of a typical incident response flow.

It is important to note that the process of detection, analysis and remediation is generally going to be a cyclical process. IT and security teams will want to focus first on critical assets that have been identified prior to the high-impact vulnerability in the preparation phases. They should then work through the rest of the assets. Teams should also continuously monitor the entire network for a reintroduction of the vulnerability, especially after new devices are added to the network.

Post-Incident and Forensics

Once the fire drill of identifying and remediating systems is completed, it is important to meet with the team to clearly identify the issues the organization faces in terms of people, process and technology. Usually, this is a good time to identify which processes or tasks can be automated in the future, particularly around detection and analysis. Automating data collection allows this information to be provided to security teams much more quickly, and the remediation processes can occur faster as well.

Conclusion

High-impact vulnerabilities have become the new norm, and IT and security teams should have a strategy in place to deal with them. Organizations should leverage the existing controls, processes and tools they already use within their organization to mitigate the risk and reduce response times to these threats. Focusing on the first five Controls is a great foundation for a program designed to effectively manage the risk associated with high-impact vulnerabilities. These controls are primarily preparatory and preventive, but they form the basis of your incident response plan and make it possible to quickly and effectively identify and remediate vulnerable systems. Without these controls in place it's impossible to close the threat gap.

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

WPRHIV2b 1808