SOLUTION BRIEF

Advanced Vulnerability Risk Scoring and Prioritization

Tripwire is the leading global provider of risk-based security and compliance management solutions that enable organizations to effectively connect security to the business.

Over the past several years, the number of known vulnerabilities has grown drastically, and has continued to challenge security and operations teams to keep pace with the continuing flow of new security advisories. One of the biggest problems is accurately determining which vulnerabilities present the greatest risk to prioritize remediation efforts.

Most vulnerability management tools use crude measurements of vulnerability risk such as Low, Medium and High. Even Microsoft uses just Low, Moderate, Important and Critical to characterize their advisories. Unfortunately, some "Criticals" are much more risky than others, and you probably have tens of thousands of vulnerabilities to address in your network. Without a lot of time-consuming analysis, it's impossible to know where to start.

To address this problem, Tripwire has developed the Vulnerability Risk Score. This score combines three key vulnerability attributes in a computation that estimates the risk of a vulnerability. These scores can range from zero to greater than 50,000, giving you the most precise metric for vulnerability prioritization available today.

How is the Vulnerability Risk Score computed?

The Tripwire Vulnerability Risk Score is computed based on parameters

that are assigned to each vulnerability by Tripwire VERT (Vulnerability and Exposure Research Team). When VERT adds coverage for a vulnerability, an in-house researcher analyzes the vulnerability and assigns Risk Class and Skill Level parameters to it. These parameters are factored with Vulnerability Age in an equation that computes the Vulnerability Risk Score.

Risk Class

Risk Class reflects the consequences of a successful exploit of the vulnerability, the requirement for user involvement in the exploit, and the prevalence of the targeted application.

The following scale is used to measure the Risk Class:

1. **Exposure.** Any externally-accessible service or application (e.g., Telnet or FTP) is a target for an attacker. Unnecessary services should be disabled to minimize the target surface of each host.
2. **Local Availability.** A vulnerability that, with a user's assistance, permits Information about a host to be disclosed that may guide future targeted attacks, but do not directly provide access to the host.
3. **Local Access.** A vulnerability that, with a user's assistance, provides some level of access to a host but not complete control.
4. **Local Privileged.** A vulnerability that, with a user's assistance, provides complete control of the host, such as some Microsoft Office vulnerabilities.
5. **Remote Availability.** A vulnerability that permits a remote attacker to obtain information about a host that might guide future targeted attacks, but does not directly provide access to the host.
6. **Remote Access.** A vulnerability that permits a remote attacker to obtain some level of unprivileged access to a host, such as a Guest account with a weak password.
7. **Remote Privileged.** A vulnerability that permits a remote user to obtain complete control of the host. Since malware is increasingly targeting host applications like browsers and Adobe Reader, highly-targeted vulnerabilities of widely-used applications are included in this category to reflect the severity of the risk.

CVE ID	VULNERABILITY	CVSS SCORE	TRIPWIRE GRANULAR RISK SCORING
CVE-2008-4250	MS08-067: Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability	10	25117
CVE-2010-2965	Wind River VxWorks WDB Agent Debug Service Remote Access Breach Vulnerability	10	17174
CVE-2008-0960	Apple Mac OS X Net-SNMP Remote Authentication Bypass Vulnerability	10	2941
CVE-2010-3972	MS11-004: Microsoft IIS FTP Service Heap Buffer Overrun Vulnerability	10	930
CVE-2008-3146	CESA-2008:0890 Wireshark Buffer Overflow	10	118
CVE-2008-5412	IBM WebSphere Application Server JSP unspecified Vulnerability	10	0

Fig. 1 The Tripwire Vulnerability Risk Score clarifies the relative risk of several vulnerabilities with an identical CVSS score of 10.

Skill Level

Skill Level reflects the likelihood of an exploit based on the availability and sophistication of exploit methods and tools "in the wild." The following scale is applied to the Skill Level of a vulnerability:

1. **Automated Exploit.** Exploit methods that automatically seek vulnerable hosts and exploit the vulnerable application automatically.
2. **Easy.** A "point-and-shoot" exploit that requires little or no technical knowledge to achieve a successful attack.
3. **Moderate.** An unsophisticated exploit tool that requires relatively basic technical knowledge to be successful.
4. **Difficult.** A very basic exploit tool that requires some knowledge of operating systems, shell code, interpreters, or networking to be successful.
5. **Extremely Difficult.** "Proof-of-concept" exploit tools exist that require detailed knowledge of compilers, operating systems, or network protocols to implement.
6. **No Known Exploit.** No successful exploits have been detected (yet) in the wild.

Vulnerability Age

Vulnerability Age is the third parameter used in computing the Tripwire Vulnerability Risk Score. Numerous studies by SANS, the FBI and others have shown that a large proportion of system and network compromises have begun with successful attacks against very old vulnerabilities. Older, well-known vulnerabilities are the low-hanging fruit that are most widely targeted by automated malware tools. The Vulnerability Risk Scores increase significantly over time to reflect this progressive risk.

Host Scores and Average Host Scores

Tripwire® IP360™ adds the total of the Vulnerability Risk Scores for each host to calculate its Host Score. This single number tells you at a glance the overall level of vulnerability risk for the host. Tripwire IP360 also computes the Average Host Score for any selected group of hosts and can present trend graphs for Average Host Score over time. The Host Scores and Average Host Scores are key metrics for monitoring the effectiveness of your vulnerability risk management program.

Conclusion

The Tripwire Vulnerability Risk Scores, Host Scores and Average Host Scores help you prioritize and manage vulnerability risks in your network. By focusing remediation efforts on the highest risk hosts and the highest scoring vulnerabilities, you can achieve the greatest possible risk reduction with available resources. These scores provide a standardized and proven set of metrics for managing and monitoring the vulnerability remediation workflow process.

tripwire®

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

©2019 Tripwire, Inc. Tripwire, Log Center/LogCenter, IP360 and Tripwire Axon are trademarks or registered trademarks of Tripwire, Inc. All other product and company names are property of their respective owners. All rights reserved.
SBAVRSP1j 1307