# Practical Implementation of CVSS

By Justin Hall and Mike Schuetter

**To properly inform and support these groups, security operations teams are realizing that an organized vulnerability rating system must be deployed — providing the ability to classify, prioritize, and score new vulnerabilities in a consistent fashion.**

Ask any information security professional what issues he or she faces on a daily basis and it is likely that the topic of vulnerability management will top the list. Patching timelines have accelerated. The time between vulnerability announcement and exploit code appearance has continued to shrink. With an already overloaded staff, patch management teams are constantly seeking ways to prioritize their work to best remediate known vulnerabilities and reduce a company's overall exposure.

To assist in this endeavor, it is not uncommon for a typical security analyst, monitoring mailing lists like Bugtraq and sites like SANS' Internet Storm Center, to receive and research a dozen alerts daily that describe newly discovered vulnerabilities. The analyst will then spend a significant amount of time separating the proverbial wheat from the chaff. From all the information received, they must quickly perform the daunting task of identifying which of the vulnerabilities are relevant to the organization they protect, and from that list, which ones require immediate attention.

Once a critical vulnerability is identified for a particular organization, both its description and severity, and the company's overall exposure, must be effectively communicated to both executive management and remediation teams in a well-understood format. To properly inform and support these groups, security operations teams are realizing that an organized vulnerability rating system must be deployed—providing the ability to classify, prioritize, and score new vulnerabilities in a consistent fashion.

## Key Requirements of a Vulnerability Rating System

When considering a vulnerability rating system, there are several key components that are necessary to ensure its effectiveness:

**Comprehensive**—The rating system must take into consideration a variety of inherent characteristics in the vulnerability itself, yet be customizable to include the relative exposure of the organization in question.

**Universal**—The rating system must have the ability to be applied to any and all vulnerabilities found in the environment.

**Straightforward**—With the discovery of new vulnerabilities on a daily basis, the system must be fast and efficient. The output must be easily understood by both technical personnel and upper level management alike. The ratings must provide enough supporting evidence to establish priority in the company's remediation processes.

**Time sensitive**—Over time, it is expected that a particular rating will change based on key events—such as the release of exploits in the wild, vendor response, or continued remediation work performed on-site.

**Consistent**—Lastly, it is important that the system provide a consistent rating for all types of vulnerabilities, allowing for an "apples to apples" comparison when determining its overall remediation priority.

The Department of Homeland Security's National Infrastructure Advisory Council (NIAC) believed that such a system was necessary as well. The NIAC developed the Common Vulnerability Scoring System (CVSS) based on similar requirements as mentioned above. Its primary purpose was to develop an open and comprehensive rating system to be ubiquitously used across the industry. It would standardize how vulnerabilities are scored by all organizations. Although the NIAC developed the CVSS, its custodianship was given to the Forum of Incident Response and Security Teams (FIRST) in 2005.

The CVSS seems to be gaining traction. The current list of adopters on www.first.org is increasing in size and includes companies such as Symantec, Cisco, US-CERT, and NIST. These organizations are either testing the system's usability, or have actually begun using the system in production.

**The CVSS seems to be gaining traction. The current list of adopters includes companies such as Symantec, Cisco, US-CERT, and NIST.**

## The System Basics

The CVSS creates a composite of three scores, each of which is determined by its own set of variables. Although the original reference

is located at www.first.org/cvss, a description of each of these scores along with real-world examples can be found below.

## The Base Score

The Base score represents those aspects of the particular vulnerability that remain constant. For most vulnerabilities, it is expected that the vendor or manufacturer of the impacted system will provide this score or a bulletin with sufficient information to allow others to easily generate the score. It takes into account the following variables:

- Access Vector: Is the vulnerability remotely exploitable, or does it require local access to the system? For example, the Windows LSASS buffer overflow vulnerability would be rated "remote" since it can be exploited by an attacker sending packets at a target system across a network connection.
- Access Complexity: Is the vulnerability difficult to exploit? A rating of "low" generally means that, once a vulnerable system is identified by an attacker, the actual attack is fairly trivial. If other barriers were in place (e.g., the attack could only occur at a specific time, or a certain service would need to be disabled first), a rating of "high" would be appropriate.
- Authentication: Is authentication necessary to successfully attack the system? The Windows WMF vulnerability would receive a "not required" rating. While a logged-on user must open a malicious WMF file, the vulnerability itself does not require that any additional authentication take place to be successfully exploited.
- Confidentiality Impact: Does exploitation of the vulnerability result in a compromise in the confidentiality of information? Three ratings are possible in this parameter:
- A rating of "none" means there is no impact on confidentiality.
- A rating of "partial" means that some, but not all, confidential material on the target system is available to the attacker.
- A rating of "complete" means that all data on the system is available to an attacker. Any vulnerability that allows for privilege escalation would likely receive this rating.
- Integrity Impact: Does exploitation of the vulnerability result in a compromise of the integrity of information? This is similar to the Impact Confidentiality rating.
- Availability Impact: Does exploitation of the vulnerability result in a compromise of the availability of information? This also is similar to the Confidentiality Impact rating.
- Impact Bias: Does the vulnerability affect any one of the confidentiality, integrity, or availability of information more than the others? For instance, a vulnerability that results in a denial of service could impact availability much more than integrity or confidentiality.

## The Temporal Score

The Temporal score measures the characteristics of the vulnerability that do not remain constant over a period of time. Detail on these factors should also be driven by vendors or security-focused organizations. Variables utilized to determine this score include:

- Exploitability: What is the current likelihood of exploitation of the vulnerability? Does exploit code exist in the wild? As an example on scoring this variable, the bulletin detailing the Windows Plug and Play buffer overflow was released on August 9, 2005. At that time, it would have been rated as "unproven." In the following days, proof-of-concept code was released, followed closely by actual exploit code, and finally malware. At each step the rating would have escalated until it eventually reached "high."
- Remediation Level: What protection is in place to defend against exploitation of the vulnerability? Is there a vendor workaround or an official patch? When the Windows WMF vulnerability was first discovered in December 2005, it would have been rated as "unavailable." Eventually a non-official patch was released, followed by an official workaround from Microsoft, and finally an official patch. At each step, the rating would have changed, until it eventually reached "official fix."
- Report Confidence: What certainty exists that the vulnerability is legitimate? Has the vendor released a bulletin? Was it discovered by a single user whose story is unconfirmed, or has it been reported from multiple, credible sources? For example, some Internet Explorer vulnerabilities, while discovered and verified by credible sources, do not have official bulletins from Microsoft, rating them as "uncorroborated."

## The Environmental Score

The Environmental score measures a vulnerability's impact to a particular organization based on the technical aspects of the customer's computing infrastructure in question. Variables utilized in determining this final score include:

- Collateral Damage Potential: What is the potential for loss of life, or property, financial or physical damage? For example, if the vulnerability could cause damage to the surface of the physical disk on the target system, it would likely rate as "low."

**An analyst should make use of the three separate scores to highlight the specific factors that create risk for the organization when communicating the severity of the vulnerability.**

- Target Distribution: What percentage of the environment is affected by the vulnerability? A vulnerability in Apache would likely receive a lower rating in an organization mostly running Microsoft servers, whereas a vulnerability in IIS would rate higher in that same environment.

## What Do the Scores Mean?

Although each of the scores builds upon the others into a single composite score, an analyst should make use of the three separate scores to highlight the specific factors that create risk for the organization when communicating the severity of the vulnerability.

A high Base score indicates that the technical aspects inherent to the vulnerability have caused significant risk. Most likely it is simple to exploit and can be performed remotely without authentication. This may lead a team to question the risk of continuing use of a technology or a product that can so easily be compromised.

A high Temporal score in a fairly new vulnerability is usually indicative of a technology that has gained widespread acceptance and as a result has a significant base of potential targets—because malicious users stand to benefit from the creation of a working exploit. Most high-profile vulnerabilities will likely end up with the same Temporal score—with some functional or sophisticated exploit code available, an official notification from the vendor, and a working patch to remediate the issue.

A high Environmental score indicates that the customer's environment has a high exposure to potential exploit. A consistent number of vulnerabilities that have a high Environmental score may indicate an issue with the defenses put in place by IT teams, such as a poor patch management system or a lack of key executive support for a fully functional security program.

Once assessed, information about the vulnerability, its scores, and a remediation plan can be distributed to the appropriate remediation teams. These scores allow the teams to objectively prioritize their patch management strategy and to address those vulnerabilities that scored the highest in an effort to best mitigate the company's overall risk. Regular updates should also be communicated as the associated factors listed above modify the scores associated with the vulnerability.

**Scores allow the teams to objectively prioritize their patch management strategy and to address those vulnerabilities that scored the highest in an effort to best mitigate the company's overall risk.**

Many online tools are available to assist with the calculation of the CVSS score. NIST's Web-based CVSS calculator, used to determine scores for NIST's National Vulnerability Database, is a fast and easy method to rate a given vulnerability. It is available here: http://nvd.nist.gov/cvss.cfm?calculator. FIRST also has an extensive guide that covers more of the quantitative pieces of the CVSS. It is available here: http://www.first.org/cvss/cvss-guide.html.

## A Hypothetical Scenario

Let's examine a hypothetical scenario to illustrate everyday usage of the CVSS:

Assume that you are a security analyst on the incident response team for a medium-sized company. The company has a 1000-system network, of which 800 are end-user PCs that run Microsoft's Windows XP operating system, and 50 are servers running Windows 2000 Server. The last 150 represent an assortment of infrastructure components and miscellaneous server operating systems. A security research firm releases a bulletin concerning a vulnerability found in the Internet Explorer Web browser. The vulnerability allows code execution with escalated privileges through a buffer overflow that had been discovered. Very little information is posted as yet abou how to exploit the vulnerability. It affects all supported versions o Internet Explorer.

Given these criteria, one would use the following values to calculat the score:

Base:

- Access Vector: Remote
- Access Complexity: Low
- Authentication: Not Required
- Confidentiality: Complete
- Availability: Complete
- Integrity: Complete
- Bias: Normal
- Temporal:
- Exploitability: Unproven
- Remediation Level: Unavailable
- Report Confidence: Unconfirmed

Environmental:

- Collateral Damage: Low—other than physical hard disks taking damage, no potential for physical damage exists
- Target Distribution: High (76% - 100%)

At this point, using the NIST calculator, the vulnerability rates:

- Base score: 10
- Temporal score: 7.7
- Environmental score: 7.9
- Overall score: 7.9

The Base score is at its maximum of 10 due to the simplicity of the exploit and the ability to execute code at a high privilege level—which leads to the high impact on confidentiality, integrity and availability. The Base score will never change throughout the life of this vulnerability. The lack of working exploit code and a confirmation from the vendor leads to a lower Temporal score. Due to the high number of potentially vulnerable systems, the Environmental score and therefore the final composite score are slightly higher.

Now assume that a few days later, several other security research firms have released bulletins of their own with similar findings. This leads Microsoft to release their own official bulletin containing instructions for a workaround that would prevent the attack. In addition, proof-of-concept code has been publicly released and is being actively distributed. The following parameters have changed:

- Exploitability: Proof-of-concept code
- Remediation Level: Workaround
- Report Confidence: Confirmed

This changes the Temporal score to 8.6, modifies the Environmental score to 8.7, and gives it a new overall score of 8.7.

Continuing with this example, assume that associated exploit code is now found on several Web sites, and URLs of those Web sites are being distributed via mass email and instant messaging bots. Microsoft releases a patch for the vulnerability and you begin deployment; however, your patch management system only reaches 50 percent of your environment in the first day.

The following parameters have changed:

- Exploitability: High
- Remediation Level: Official fix
- Target distribution: Medium (26%-75%)

This changes the Temporal score to 8.7. The Environmental score drops to 6.6 due to your patching efforts. From this point forward, it is unlikely that the Temporal score will change (unless a problem is found with the official fix that causes the vendor to retract it). Further changes to the Environmental score will only occur due to your ongoing and successful patching efforts. Once you reach the threshold of 90 percent of systems patched, the Environmental score (and subsequently the overall score) will drop to 2.2.

**Whether CVSS will become a true industry standard has yet to be seen. In the meantime, security teams can find merit in the overall system.**

## Final Thoughts

IT security teams constantly look to standards from groups like NIST, CERT, ISO and the National Infrastructure Advisory Council for guidance. While not all standards are a perfect fit, most of these can be tuned to meet an organization's needs. In the end, they set a direction and foundation upon which to build a security framework suited for a particular company.

This document has outlined the Common Vulnerability Scoring System and provided real-world examples to show its usefulness. The concept of three scores that focus on various aspects of any given vulnerability provides great insight into that vulnerability's core characteristics and the urgency that should be placed on remediating it. Security operations teams may wish to modify the variables or their values slightly to better meet their own needs, but overall the system meets all of the initial requirements set forth in this article.

Whether or not CVSS will become a true industry standard is yet to be seen. In the meantime, security operations teams can find merit in the overall system and can utilize it for their own framework to deliver a common and consistent message to management and remediation teams alike.

## About the Authors

*Justin Hall (Justin.Hall@cbts.cinbell.com) is a Senior Security Engineer at CBTS, an IT services and outsourcing division of Cincinnati Bell. He is currently serving as a lead research and incident response security analyst for a large manufacturing company.*

*Mike Schuetter, CCIE, CISSP (Michael.Schuetter@cbts.cinbell.com), is a Senior Manager at CBTS and is currently serving with Mr. Hall as the Security Operations Manager.*