October 2007

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

THE COMMON VULNERABILITY SCORING SYSTEM (CVSS)

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

To protect the security of their information technology (IT) systems, managers must continually identify and assess the vulnerabilities of their systems. Severe weaknesses in IT systems security often stem from software or system implementation flaws. These weaknesses, or vulnerabilities, make the systems attractive targets for attacks that can seriously change or harm the confidentiality of data, the integrity of data, and the availability of systems. Because they may have many different hardware and software platforms and many different threat issues to deal with, managers need a way to prioritize the vulnerabilities of their systems and to address those vulnerabilities that pose the greatest risk.

The Information Technology Laboratory of the National Institute of Standards and Technology (NIST) recently issued information about the Common Vulnerability Scoring System (CVSS), which provides an open framework for scoring the characteristics and impacts of IT vulnerabilities. The CVSS enables IT managers, vendors, information providers, and researchers to exchange information about IT vulnerabilities using a common language and scoring scheme, and to take needed actions to improve the security of their systems.

NISTIR 7435, *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems*

The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems, written by Peter Mell and Karen Scarfone of NIST and by Sasha Romanosky of Carnegie Mellon University, was issued in August 2007 as NIST Interagency Report (NISTIR) 7435. The report explains the CVSS and discusses the available methods and issues related to scoring systems for vulnerabilities.

NISTIR 7435 helps IT managers to make sense of vulnerability data and to take appropriate actions that will protect their systems and information. NISTIR 7435 describes in detail the three groups of metrics that compose the CVSS and provides specific examples of how to perform the CVSS scoring procedures. It provides guidelines on the scoring process and defines the equations used to generate three groups of metrics: base, temporal, and environmental scores. Also included in the report are examples of the scoring to help explain the process and the use of the equations.

The appendices provide information about electronic in-print resources that are available to help organizations implement the CVSS. Also included in the appendices are an abbreviation list and an acronym list. NISTIR 7435 is available from NIST's website at http://csrc.nist.gov/publications/nistir/ir7435/NISTIR-7435.pdf.

Scoring for Vulnerabilities

Both commercial and noncommercial organizations have developed vulnerability "scoring" systems that are available for use. These various systems have different advantages and disadvantages, and they often differ in what they measure. Some of these scoring systems provide only one approach for measuring the impact of vulnerabilities, and they may assume that the impact of vulnerabilities is uniform for all individuals and organizations.

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since September 2006:

The CVSS provides a more consistent approach to scoring vulnerabilities. It is managed by the Forum of Incident Response and Security Teams (FIRST), an international confederation of computer incident response teams that handle computer security incidents and promote incident prevention programs. The CVSS is a free and open standard, is available to all to use and implement, and is not limited just to members of FIRST. To further common understanding of the scores that users obtain with the CVSS, FIRST asks that organizations publishing vulnerability scores conform to the guidelines described in NISTIR 7435 and provide both the score and the scoring vector in their published results.

The CVSS is useful for organizations such as:

- Producers of vulnerability bulletins in both nonprofit and commercial organizations that provide CVSS temporal scores to users;

- Software application vendors who provide CVSS information to their customers to enable them to manage their IT risks more effectively;

- Private sector organizations that use the CVSS internally to make informed vulnerability management decisions;

- Vulnerability scanning and management organizations that scan networks for IT vulnerabilities and make CVSS scores available to user organizations;

- Security risk management firms that use CVSS scores as input to report to their customers about their risk or threat levels; and

- Researchers who perform statistical analyses on vulnerabilities and vulnerability properties.

The Common Vulnerability Scoring System version 2.0 website is at http://www.first.org/cvss/cvss-guide.html.

The Scoring System

The CVSS consists of three groups of scores: Base, Temporal, and Environmental. Each group produces a numeric score ranging from 0.0 to 10.0 and a vector, a compressed textual representation that reflects the values of the metrics used to derive the score.

The **Base** group of metrics represents the intrinsic and fundamental characteristics of a vulnerability that are constant over time and user environments.

The **Temporal** group represents the characteristics of a vulnerability that change over time but not among user environments.

The **Environmental** group represents the characteristics of a vulnerability that are relevant and unique to a particular user's environment.

The detailed process for scoring is explained in Section 3 of NISTIR 7435. Scoring can be done by any of the user organizations mentioned above. In general, vulnerability bulletin analysts, security product vendors, and application vendors, with detailed knowledge of the characteristics of vulnerabilities, usually cite the base and temporal metrics. If they desire, users can use the CVSS to check a vendor's calculations of vulnerabilities. Users generally cite the environmental metrics because they are best able to assess the potential impact of a vulnerability within their own environments.

There are clear benefits to be gained from using the CVSS, which allows managers to convert masses of vulnerability data into distilled information that they can directly apply to improve the security of systems. Specific benefits include:

Standardized Vulnerability Scores: When an organization normalizes vulnerability scores across all of its software and hardware platforms, it can leverage a single vulnerability management policy. This policy may be similar to a service level agreement (SLA) that states how quickly a particular vulnerability must be validated and remediated.

Open Framework: Users can see the individual characteristics that are used to derive a score for a vulnerability when the CVSS is used. This common framework helps to avoid user confusion when a vulnerability is assigned an arbitrary score under a different system.

Prioritized Risk: When the environmental score is computed for a vulnerability, users can put the information into the context of their systems, determine the actual risk that the vulnerability poses, and judge the impact of the vulnerability in relation to other vulnerabilities.

Who We Are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

The CVSS and the National Vulnerability Database (NVD)

The NIST National Vulnerability Database (NVD) is a comprehensive cyber security vulnerability database that integrates all publicly available federal government vulnerability resources and provides references to industry resources. The NVD website is http://nvd.nist.gov/. The NVD is based on and synchronized with the Common Vulnerabilities and Exposures (CVE) vulnerability dictionary of software flaws. NVD provides vulnerability summaries for all CVE vulnerabilities. The NVD includes a fine-grained search engine that allows users to search for vulnerabilities by various characteristics.

The NVD provides specific CVSS scores for publicly known vulnerabilities. With this link, the NVD provides valuable information to information system managers, users, system administrators, and other security professionals to help them learn about vulnerabilities and take steps to correct them.

For all of the vulnerabilities that are listed, NVD uses the scoring guidelines detailed in NISTIR 7435 to create CVSS base metric scores. A CVE identifier is assigned to each new vulnerability. NVD

analysts review the new vulnerability, assign a CVSS base score, and add the information to the corresponding CVE entry within the database. The CVSS base scores in the NVD are available for use by federal agencies, so that they do not have to manually calculate their own base scores. These scores are also incorporated into many commercial security tools. Agencies may wish to ask their security tool vendors if they provide the NVD CVSS scores within their products. NVD is publicly available, so any organization or individual may freely use its CVSS base scores. The NVD CVSS web page is available at http://nvd.nist.gov/cvss.cfm.

Having the base metric score listed for each CVE entry in NVD enables users to quickly determine the severity of each vulnerability. However, when the temporal and environment metrics are missing, an incomplete picture may result. To remedy this, NVD provides a web-based CVSS version 2.0 calculator at the web page listed above.

When users select a vulnerability from the NVD and click on the "Base score" attribute, they are directed to the calculator and the base metric scores will be filled in automatically, leaving the temporal and environmental metrics to be completed by the user. The Base metrics can be altered by users to suit their specific needs should they wish to do so. Once all the information has been submitted, users are presented with an adjusted score that more directly reflects the impact of the vulnerability on their environment. Commercial tools may also offer the ability to customize NVD CVSS base scores with environment-specific information.

CVSS was designed to be used by any organization. This flexibility is a noteworthy strength of the system, but it does require that different sectors and organizations approach the use of CVSS with consideration of their specific requirements.

Modifying Scores with FIPS 199 Ratings

The Federal Information Security Management Act (FISMA) of 2002 requires all federal agencies to develop, document, and implement agency-wide information security programs and to provide information security for the information and information systems that support the operations and assets of the agency, including those systems provided or managed by another agency, contractor, or other source. To help agencies carry out these policies, FISMA called for NIST to develop federal standards for the security categorization of federal information and information systems according to risk levels and for minimum security requirements for information and information systems in each security category. Federal Information Processing Standard (FIPS) 199, *Standards for the Security Categorization of Federal Information and Information Systems*, issued in February 2004, was the first standard that was specified by FISMA. FIPS 199 requires agencies to categorize their information systems as low-impact, moderate-impact, or high-impact for the security objectives of confidentiality, integrity, and availability.

Federal agencies can use the following FIPS 199 security categories with the NVD CVSS scores to obtain impact scores that are tailored to each agency's environment.

The potential impact is **low** if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.

The potential impact is **moderate** if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.

The potential impact is **high** if the loss of confidentiality, integrity, or availability could be expected to have a **severe** or **catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

The CVSS generally follows the FIPS 199 definitions for the impact subscore modifiers in the environmental metric, so federal agencies can customize CVSS scores to apply to specific government systems. However, CVSS does not require that these definitions be used by all and provides them merely as a default; other organizations using the CVSS may choose to define the impact subscore modifiers in ways that more closely suit their particular business goals.

For federal agencies, the FIPS 199 definitions can apply, and the potential impact levels for federal information systems can be considered when agencies are calculating environmental metric scores for vulnerabilities. For example, an information system may have potential impact levels of high for confidentiality and integrity, and moderate for availability according to the FIPS 199 definitions of potential impacts. These values can then be input into the CVSS calculator for the environmental metric impact subscore modifiers. Once these values have been entered, the final CVSS score will be adjusted appropriately, resulting in a CVSS score that is specifically tailored to the target environment. However, a CVSS score only assesses the relative severity of a vulnerability when compared to other vulnerabilities and does not take into account any security controls that might mitigate attempts to exploit the systems, such as firewalls, antivirus software, intrusion detection and prevention systems, and authentication mechanisms. CVSS scores are intended as an aid in making decisions about security controls and are only one element of many factors that should be considered.

Using CVSS with Security Content Automation Protocol

The Security Content Automation Protocol (SCAP) is a method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation, such as FISMA compliance. Specifically, SCAP is a suite of selected open standards that enumerate software flaws, security-related configuration issues, and product names; measure systems to determine the presence of vulnerabilities; and provide mechanisms to rank (score) the results of these measurements to evaluate the impact of discovered security issues. SCAP defines how these standards are combined. CVSS is one of the six vulnerability management standards that compose SCAP. More information on SCAP and how it benefits federal agencies and other organizations is available at http://nvd.nist.gov/scap.cfm.

Recommendations for Using the CVSS

NIST recommends that federal agencies and other organizations adopt the Common Vulnerability Scoring System (CVSS), which provides a standard method to rate the severity of vulnerabilities within their systems. The National Vulnerability Database (NVD) provides a standard set of federal government-validated CVSS scores. Together, when incorporated into security products, the NVD and the CVSS enable organizations to understand the impact of the vulnerabilities on their systems. Furthermore, the impact ratings will be the same even when the vulnerabilities are discovered by multiple security tools used in different organizations. This allows for a dependable comparison of the severity of vulnerabilities between federal government systems and between the government and other organizations. By watching the CVSS scores of discovered vulnerabilities over time, organizations can more easily identify vulnerability trends. Then with an effective security program implemented, organizations will see improvements in their vulnerability metrics over time.

More Information

NIST publications assist organizations in planning and implementing a comprehensive approach to information security. For information about NIST standards and guidelines that are referenced in the CVSS guide, as well as other security-related publications, see NIST's web page at http://csrc.nist.gov/publications/index.html

Publications specifically related to the CVSS include:

NIST Special Publication (SP) 800-51, *Use of the Common Vulnerability and Exposures (CVE) Vulnerability Naming Scheme*, advises federal agencies to acquire and use security-related IT products that are compatible with the CVE vulnerability naming scheme, and to periodically monitor their systems for applicable vulnerabilities, using automated software tools.

NIST SP 800-40, version 2.0, *Creating a Patch and Vulnerability Management Program*, provides guidance on management practices that can prevent the exploitation of IT vulnerabilities.

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

ITL Bulletins via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.