October 2005

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

NATIONAL VULNERABILITY DATABASE: HELPING INFORMATION TECHNOLOGY SYSTEM USERS AND DEVELOPERS FIND CURRENT INFORMATION ABOUT CYBER SECURITY VULNERABILITIES

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

The National Vulnerability Database (NVD) is a comprehensive database of cyber security vulnerabilities in information technology (IT) products that was developed by the National Institute of Standards and Technology (NIST) with the support of the National Cyber Security Division (NCSD) of the U.S. Department of Homeland Security. Integrating all publicly available U.S. Government vulnerability resources and including references to industry resources, the NVD is updated hourly to provide the latest information about vulnerabilities in IT products. The NVD is based on and is synchronized with the Common Vulnerabilities and Exposures (CVE), a vulnerability naming standard that was jointly developed by government, industry and research organizations. NVD provides a fine-grained search engine and database for assisting those using the CVE standard.

Vulnerabilities are software or system implementation flaws that can cause serious weaknesses in the security of systems. These weaknesses help to make systems attractive targets for attacks that can seriously change or harm the confidentiality of data, the integrity of data, and the availability of systems. The NVD provides valuable information to system managers, users, system administrators, and other security professionals to help them learn about vulnerabilities and take steps to correct them.

Features of the NVD

The National Vulnerability Database (NVD) is available on NIST's website at http://nvd.nist.gov. In mid-October, the NVD contained information on more than 12,800 vulnerabilities. About ten new vulnerabilities are discovered every day. The NVD can be used to research the vulnerability history of a product and to view vulnerability statistics and trends.

The NVD complements the suite of vulnerability management services that the NCSD has made available by including all publicly known

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 June 2004:

- *Information Technology Security Services: How to Select, Implement, and Manage,* June 2004
- *Guide for Mapping Types of Information and Information Systems to Security Categories*, July 2004
- *Electronic Authentication: Guidance for Selecting Secure Techniques*, August 2004
- *Information Security Within the System Development Life Cycle*, September 2004
- *Securing Voice Over Internet Protocol (IP) Networks*, October 2004
- *Understanding the New NIST Standards and Guidelines Required by FISMA, November 2004*
- *Integrating IT Security into the Capital Planning and Investment Control Process, January 2005*
- *Personal Identity Verification (PIV) of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201 Approved by the Secretary of Commerce*, March 2005
- *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,* April 2005
- *Recommended Security Controls for Federal Information systems: Guidance of Selecting Cost-effective Controls Using a Risk-based Process, May 2005*
- *NIST's Security Configuration Checklists Program for IT Products,* June 2005
- *Implementation of FIPS 201, Personal Identify Verification (PIV) of Federal Employees and Contractors, August 2005*
- *Biometric Technologies: Helping to Protect Information and Automated Transactions in Information Technology Systems, September 2005*

vulnerabilities. NCSD's other vulnerability management products focus only upon the most critical subset of vulnerabilities. For each vulnerability, NVD provides reference information and links to other government and industry resources.

NVD also integrates all publicly available U.S. Government vulnerability resources and includes references to many industry resources as well. The NVD provides direct access to United States Computer Emergency Readiness Team (US-CERT) vulnerability resources, including US-CERT Technical Alerts and Vulnerability Notes. It also provides a search engine for the Open Vulnerability and Assessment Language (OVAL).

The entire NVD database can be downloaded for public use as an XML feed from the NVD Download and Product Integration Page. This feature enables developers to easily include this information within their IT security products. NVD information, from the NIST site, is available with no licensing restrictions. However, NIST appreciates credit when appropriate within products, services, and reports that use the data, and NIST welcomes information about how users are employing the data.

Users can search the NVD by employing different vulnerability characteristics, including:

- vulnerability severity,
- software name and version number,
- vendor name,
- vulnerability type,
- vulnerability impact, and
- related exploit range.

In their searches, users may ask for those alerts that have been the subject of US-CERT Technical Alerts, US-CERT Vulnerability Notes, and OVAL queries.

Another useful feature of the NVD is support for generating statistics. The database can be used to graph and chart vulnerabilities discovered within a product or to graph and chart sets of vulnerabilities containing particular characteristics, such as remotely exploitable buffer overflows.

NIST contact information for the NVD is available at http://nvd.nist.gov/contact.cfm.

Vulnerabilities and the CVE

Vulnerabilities are flaws that can be exploited by a malicious entity to gain access or privileges that are greater than those that are authorized on an information system. Many organizations use commercial off-the-shelf security products and services to track, detect, or counter known vulnerabilities. If these products use different names for the same vulnerabilities, it is difficult to share information about vulnerabilities between the databases and tools of the different products and services.

The CVE helps to overcome this problem by providing a standard name and standard description for each vulnerability or exposure. Currently identified compatible products and services are listed on the Compatible Products pages on the CVE website: http://cve.mitre.org/compatible/.

NIST recommends that CVE data be accessed from within the NVD as more information is available about vulnerabilities from within the NVD. CVE standards information is available at http://cve.mitre.org.

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.

NIST Guidance on Use of CVE

NIST Special Publication 800-51, *Use of the Common Vulnerability and Exposures (CVE) Vulnerability Naming Scheme*, by Peter Mell and Tim Grance, September 2002, provides guidance on the use of the CVE within the federal government. This and other NIST publications are available at the NIST website: http://csrc.nist.gov/publications/nistpubs/index.html.

NIST SP 800-51 advises agencies to acquire and use security-related IT products that are compatible with the CVE vulnerability naming scheme. CVE-compatible products and services include vulnerability scanners, vulnerability databases, vulnerability advisory services, vulnerability patch services, most intrusion detection systems, and some firewalls. CVE compatibility is one important consideration among other requirements such as functionality, cost, performance, and architecture.

Secondly, agencies are also advised to periodically monitor their systems for applicable vulnerabilities listed in the CVE vulnerability naming scheme, using automated software tools. Since these tools may not detect all CVE vulnerabilities, system and security administrators now can use the NVD to check for new vulnerabilities. Further, agencies are advised to use the CVE naming scheme in their descriptions and communications on vulnerabilities with agency staff, industry, and the public. Common names for vulnerabilities can help to reduce confusion and improve accuracy of communications.

Related Guidance

Additional supporting guidance on managing vulnerabilities is available in NIST Special Publication 800-40, version 2.0, *Creating a Patch and Vulnerability Management Program*.

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.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900