October 2002

ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

SECURITY PATCHES AND THE CVE VULNERABILITY NAMING SCHEME: TOOLS TO ADDRESS COMPUTER SYSTEM VULNERABILITIES

Elizabeth B. Lennon, Editor, Information Technology Laboratory, National Institute of Standards and Technology

Today more than ever, timely response to vulnerabilities is critical to maintain the operational availability, confidentiality, and integrity of information technology (IT) systems. To assist federal agencies and industry respond to vulnerabilities in a timely manner, ITL recently released two new publications dealing with vulnerabilities in computer systems: NIST Special Publication (SP) 800-40, *Procedures for Handling Security Patches*, by Peter Mell and Miles C. Tracy, and NIST SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, by Peter Mell and Tim Grance. This *ITL Bulletin* summarizes these two documents on system vulnerabilities, available at http://csrc.nist.gov/publications/nistpubs/index.html.

Security Patches

Failure to keep operating system and application software up to date is a common mistake made by IT professionals. Despite extensive testing, all operating systems and applications are released with *bugs* (errors in the software) that affect security, performance, and stability. As software programs expand, the potential number of bugs grows. Many security-related bugs are generally discovered only after a large number of users start using the software, and hackers and independent testers start attempting to compromise it. Once a bug is discovered, the software manufacturer often releases a piece of software to correct the bug. This software is often called a patch, hotfix, or service pack.

Patches are released for three reasons:

- To fix faults in an application or operating system. Many hacker attacks are based on exploiting faults in the computer code of applications and operating systems. Patches are also released to correct performance or functionality problems.
- To alter functionality or to address a new security threat. An example of this is new virus definitions for an antivirus application. There was nothing "wrong" with the code of the antivirus program, but it had to be updated to detect new viruses that did not exist when the application was first released.
- To change or modify the software configuration to make it less susceptible to attacks and more secure.

Applying patches in a timely and consistent manner is critical to maintaining the operational availability, confidentiality, and integrity of IT systems. However, failure to keep operating system and application software patched is an all too common mistake made by IT professionals. New patches are released daily, and it is often difficult for even experienced system administrators to keep abreast of all the new patches.

The CERT/Coordination Center (CC) (http://www.cert.org) estimates that 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches. In an increasingly interconnected world, it is critical that system administrators keep their systems patched to the most secure level. A common misperception among some system administrators is that a firewall reduces the need for timely patching. Unfortunately, this is incorrect because a firewall generally permits some level of traffic between most

Continued on page 2

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 8901, Gaithersburg, MD 20899-8901, 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 March 2001

- *An Introduction to IPsec (Internet Protocol Security),* March 2001
- *Biometrics – Technologies For Highly Secure Personal Authentication*, May 2001
- *Engineering Principles for Information Technology Security*, June 2001
- *A Comparison of The Security Requirements for Cryptographic Modules In FIPS 140-1 and FIPS 140-2*, July 2001
- *Security Self-assessment Guide For Information Technology Systems*, September 2001
- *Computer Forensics Guidance*, November 2001
- *Guidelines on Firewalls and Firewall Policy*, January 2002
- *Risk Management Guidance for Information Technology Systems,* February 2002
- *Techniques for System and Data Recovery*, April 2002
- *Contingency Planning Guide for Information Technology Systems*, June 2002
- *Overview: The Government Smart Card Interoperability Specification,* July 2002
- *Cryptographic Standards and Guidelines: A Status Report*, September 2002

NIST National Institute of Standards and Technology • Technology Administration • U.S. Department of Commerce

WIZ, Inc. EXHIBIT - 1020
WIZ, Inc. v. Orca Security LTD.

internal and external hosts. As long as a communication channel is allowed between the internal network and the Internet or other external network, there is a risk of compromise; thus patching becomes critical.

Identifying Vulnerabilities and Applicable Patches

Vulnerabilities are weaknesses in software that can be exploited by a malicious entity to gain greater access and/or permission than it is authorized to have on a computer. Not all vulnerabilities have related patches; thus, system administrators must not only be aware of vulnerabilities and patches, but also of the need to mitigate *unpatched* vulnerabilities through other methods (e.g., workarounds, firewalls, and router access control lists).

To help address this growing problem, we recommend that organizations have an explicit and documented patching and vulnerability policy and a systematic, accountable, and documented process for handling patches. NIST SP 800-40, *Procedures for Handling Security Patches*, provides principles and methodologies for accomplishing this. One of several possible techniques is through the creation of a patch and vulnerability group (PVG). This group facilitates the identification and distribution of patches within the organization. Its duties include:

- Creating a reasonably representative organizational hardware and software inventory,
- Identifying newly discovered vulnerabilities and security patches,
- Prioritizing patch application,
- Creating an organization-specific patch database,
- Testing patches for functionality and security (to the degree that resources allow),
- Distributing patch and vulnerability information to local administrators,
- Verifying patch installation through network and host vulnerability scanning,
- Training system administrators in the use of vulnerability databases,
- Deploying patches automatically (when applicable), and
- Configuring Automatic Update of Applications (when applicable).

If organizations use the PVG approach, this does not diminish the responsibility of all systems administrators to patch the systems under their control. Each systems administrator should:

- Apply patches identified by the PVG,
- Test patches on the specific target systems, and
- Identify patches and vulnerabilities associated with software not monitored by the PVG.

Besides creating a PVG, organizations should be aware that applying patches and mitigating vulnerabilities is seldom, especially in large organizations, a straightforward process. To help with this, NIST SP 800-40 covers areas such as obtaining patches, prioritizing patches, testing patches, and applying patches. An overview of specific government patch and vulnerability resources is included. Appendices present a glossary of terms, patching resources for a variety of platforms and applications, guidance on using the NIST ICAT Metabase, commonly used vulnerability resources, and guidance on using other available tools and resources.

Recommendations for Handling Security Patches

Organizations should have an explicit and documented patching and vulnerability policy as well as a systematic, accountable, and documented set of processes and procedures for handling patches. The patching and vulnerability policy should specify what techniques an organization will use to monitor for new patches and vulnerabilities and which personnel will be responsible for such monitoring. An organization's patching process should define a method for deciding which systems get patched and which patches get installed first. It should also include a methodology for testing and safely installing patches.

When designing a process for handling patches, consider the principles that make up the PVG patching concept. Other patching variations may be acceptable, but the core concepts should be found within the chosen patching methodology. These ideas include using organizational inventories, vulnerability and patch monitoring, patch prioritization techniques, organizational patch databases, patch testing, patch distribution, patch application verification, patch training, automated patch deployment, and automatic updating of applications.

The patch process can be automated or manual; however, organizations should expect to transition to more automated methods in the future. The movement towards automated patch methods will parallel organizational plans to centralize services and standardize desktop configurations.

While patching and vulnerability monitoring can often appear an overwhelming task, consistent mitigation of organizational vulnerabilities can be achieved through a tested, prioritized, and integrated patching and remediation process. It is our hope that NIST SP 800-40 will aid those whose job is to undertake this important and difficult task.

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.

Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme

Closely related to the handling of security patches is a means to identify and organize known IT system vulnerabilities. As described in NIST SP 800-51, the Common Vulnerabilities and Exposures (CVE) vulnerability naming scheme is a dictionary of common names for publicly known IT system vulnerabilities. It is an emerging industry standard that has achieved wide acceptance by the security industry and a number of government organizations. Technical vulnerability experts from 31 industry, academia, and government organizations vote on the common names. CVE provides the computer security community with:

- a comprehensive list of publicly known vulnerabilities,
- an analysis of the authenticity of newly published vulnerabilities, and
- a unique name to be used for each vulnerability.

General CVE information is available at http://cve.mitre.org. The vulnerabilities listed in CVE can be viewed using the NIST ICAT vulnerability index at http://icat.nist.gov.

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 web site is http://www.itl.nist.gov/.

Guidelines for Use of the CVE Vulnerability Naming Scheme

1. **Federal departments and agencies should give substantial consideration to the acquisition and use of security-related IT products and services that are compatible with the CVE vulnerability naming scheme.**

   Most federal departments and agencies use commercial off-the-shelf (COTS) security products and services to track, detect, or counter known vulnerabilities. A problem with many of these products is that different products use different names for the same vulnerabilities. Without a consistent vulnerability terminology, it is difficult to compare the vulnerability coverage of such security products. Also, it may be complex to correlate alerts among databases and tools of different vendors or services.

   CVE-compatible products and services, however, use the same name for each vulnerability, thus addressing many of these coverage and correlation concerns. Therefore, it is important to consider acquiring CVE-compatible security products and services. Agencies should be careful, however, to consider CVE compatibility only for products and services that inherently make use of vulnerability names. Such products and services include vulnerability scanners, vulnerability databases, vulnerability advisory services, vulnerability patch services, most intrusion detection systems (IDSs), and some firewalls.

   Your organization's use of CVE-compatible products can assist you by

   - determining which product covers the vulnerabilities most applicable to an agency's network infrastructure; and
   - increasing the assurance that the alerts produced by the product(s) you choose will be able to be correlated with alerts from your other products and from your incident response center.

   The requirements for CVE compatibility are described at http://cve.mitre.org/compatible/requirements.html. Currently identified compatible products and services are listed on the Compatible Products pages, http://cve.mitre.org/compatible. While CVE compatibility should be an important consideration in IT security product and service acquisition, federal departments and agencies should foremost consider their overall requirements (functionality, cost, performance, architecture, etc.) when acquiring products and services.

2. **Federal departments and agencies should periodically monitor their systems for applicable vulnerabilities listed in the CVE vulnerability naming scheme.**

   NIST recommends monitoring systems for vulnerabilities included in the CVE list since it is a standardized, reviewed, and comprehensive vulnerability repository. CVE consists of both standardized and candidate vulnerabilities, and systems should be monitored for both types. Agencies should identify the CVE entries that apply to the software used in their systems and correct those vulnerabilities. Greater emphasis should be placed upon systems that are accessible from the Internet (e.g., web and e-mail servers), systems that house important or sensitive applications or data (e.g., databases), or network infrastructure components (e.g., routers, switches, and firewalls). Since it is infeasible for an organization to find and fix all vulnerabilities in every system simultaneously, organizations should carefully prioritize their monitoring and patching efforts (see NIST SP 800-40, *Procedures for Handling Security Patches*, http://csrc.nist.gov) to correct the most severe vulnerabilities on the most high-risk systems.

   Automated software tools can scan hosts and networks for CVE vulnerabilities, and we recommend regular use of such products. However, such products may not check for every CVE

vulnerability entry. For additional thoroughness, systems administrators and security officers can periodically compare the software products used on systems directly to the entries listed in the CVE repository. For complete CVE coverage, we recommend performing this comparison using the NIST ICAT Metabase (http://icat.nist.gov). ICAT is a publicly available CVE search engine that allows one to search for vulnerabilities by vendor names, products names, version numbers, and other parameters. When an applicable vulnerability is found, ICAT provides a variety of vulnerability attributes (e.g., attack range and damage potential) and links to vulnerability and patch information from a variety of public resources. In summary, NIST recommends the use of automated scanning tools on a frequent basis combined with periodic manual vulnerability discovery using ICAT.

3. **Federal departments and agencies should use the CVE vulnerability naming scheme in their descriptions and communications of vulnerabilities.**

Agencies should use CVE in their internal reports of vulnerability scans, notifications to system owners of observed vulnerabilities, and alerts identifying the vulnerabilities targeted by active exploits. Use of CVE will help to minimize confusion regarding which vulnerability is being referenced and provides an excellent check on whether the referenced vulnerability has been eliminated.

Agencies should also use CVE in communicating information about vulnerabilities externally. For example, communications to FedCIRC or other incident response teams should reference, where known, the CVE vulnerability name that newly observed exploits are targeting. Also, communications with vendors will be more accurate if CVE numbers are used. If a vendor-supplied patch that purports to fix a vulnerability is defective, a statement to the vendor that a given CVE vulnerability remains after applying the patch conveys important information clearly and succinctly. Also, communications with vendors of scanning tools regarding false positives or false negatives will be clearer if the offending vulnerability is labeled by CVE number.

In conclusion, ITL recommends the timely and consistent use of security patches and the CVE vulnerability naming scheme to mitigate the impact of vulnerabilities in computer systems. The NIST ICAT Vulnerability Metabase is a free resource which to date contains more that 5,164 known vulnerabilities. We invite you to explore this valuable tool at http://icat.nist.gov/. Finally, we acknowledge the leadership, vision, and initiative of the MITRE Corporation and the various contributors in the public and private sectors in creating, maintaining, and operating the CVE repository.

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

Official Business
Penalty for Private Use $300

Address Service Requested

PRSRT STD
POSTAGE & FEES PAID
NIST
PERMIT NUMBER G195