February 2006

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

CREATING A PROGRAM TO MANAGE SECURITY PATCHES AND VULNERABILITIES: NIST RECOMMENDATIONS FOR IMPROVING SYSTEM SECURITY

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

A systematic approach to managing and using software patches can help organizations to improve the overall security of their information technology (IT) systems in a cost-effective way. Organizations that actively manage and use software patches can reduce the chances that the vulnerabilities in their IT systems can be exploited; in addition, they can save time and money that might be spent in responding to vulnerability-related incidents.

Patches are additional pieces of code that have been developed to address specific problems or flaws in existing software. Vulnerabilities are flaws that can be exploited, enabling unauthorized access to IT systems or enabling users to have access to greater privileges than authorized.

New vulnerabilities are discovered each day, and IT systems are constantly threatened by new attacks. The National Vulnerability Database (NVD), maintained by NIST's Information Technology Laboratory, includes information about more than 16,000 vulnerabilities and reports about new vulnerabilities at the rate of 14 per day. The NVD integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources. At the current rate of vulnerability reporting, even small organizations with a single server can expect to spend considerable time reviewing and applying critical patches. Organizations must be aware of and use available security patches. Since not all vulnerabilities have related patches, however, it is essential to apply other security controls that are selected through an analysis of the vulnerabilities and the risks to systems.

NIST Special Publication 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*

NIST recently issued Special Publication (SP) 800-40, Version 2, *Creating a Patch and Vulnerability Management Program*. Written by Peter Mell of NIST, Tiffany Bergeron of The MITRE Corp., and David Henning of Hughes Network Systems LLC, NIST SP 800-40 was developed with the support of the United States

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 March 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*
- *National Vulnerability Database: Helping Information Technology System Users and Developers Find current Information About Cyber Security Vulnerabilities, October 2005*
- *Securing Microsoft Windows XP Systems: NIST Recommendations for Using a Security Configuration Checklist, November 2005*
- *Preventing and Handling Malware Incidents: How to Protect Information Technology Systems from Malicious Code and Software, December 2005*
- *Testing and Validation of Personal Identity Verification (PIV) Components and Subsystems for Conformance to Federal Information Processing Standard 201, January 2006*

Computer Emergency Readiness Team (US-CERT), an organization in the Department of Homeland Security that coordinates defense against and responses to cyber attacks. Version 2 supplements the earlier version of NIST SP 800-40, entitled *Procedures for Handling Security Patches* (August 2002). Both publications are available at: http://csrc.nist.gov/publications/nistpubs/index.html.

NIST SP 800-40 provides guidance for organizational security managers who are responsible for designing and implementing security patch and vulnerability management programs and for testing the effectiveness of the programs in reducing vulnerabilities. The guidance is also useful to system administrators and operations personnel who are responsible for applying and testing patches and for deploying solutions to vulnerability problems.

Topics covered in Version 2 include the principles and methodologies for patch and vulnerability management, security metrics for testing the effectiveness of the patch and vulnerability process, management issues such as setting priorities for patch efforts, and federal government resources available to support the patch and vulnerability processes. The appendices include a list of acronyms, a glossary of terms, and information on patch and vulnerability issues available from industry sources.

Security Patches

Timely patching of software is generally recognized as critical to maintaining the operational availability, confidentiality, and integrity of IT systems. Failure to keep operating system and application software patched is one of the most common problems that security and IT professionals must handle. New patches are released daily, and even experienced system administrators may have difficulty in keeping informed about the new patches and in deploying them properly in a timely manner.

Most major attacks on IT systems over the past few years have targeted known vulnerabilities for which patches had existed before the outbreaks. Information about patches can also lead to problems for organizations. Often when a patch is released, attackers will make concerted efforts to reverse engineer the patch swiftly (in days or even hours), to identify the vulnerability, and to develop and release code that exploits the vulnerability. As a result, the period immediately following the release of a patch can be particularly dangerous for organizations because of the time that they need to obtain, test, and deploy the patch.

NIST Recommendations for Patch and Vulnerability Management

Organizations should implement a systematic, accountable, and documented process for managing exposure to vulnerabilities through the timely deployment of patches. NIST recommends that federal agencies implement the following actions to assist in patch and vulnerability management:

Create a patch and vulnerability group (PVG) to facilitate the identification and distribution of patches within the organization.

The PVG should be specially tasked to implement the patch and vulnerability management program throughout the organization. The PVG is the central point for vulnerability remediation efforts, such as implementing patching and configuration changes for operating system and application software. Since the PVG should work actively with local administrators, large organizations may need to organize several PVGs; these groups could work together or they could be structured hierarchically with an authoritative top-level PVG.

The duties of a PVG include the following:

1. Inventory the organization's IT resources to identify the hardware equipment, operating systems, and software applications that are used within the organization.

2. Monitor security sources for vulnerability announcements, patch and non-patch methods of remediation, and emerging threats that match up with the software within the system inventory of the PVG.

3. Prioritize the order in which the organization addresses the remediation of vulnerabilities, based on analysis of risks to systems.

4. Create a database of remediation methods that need to be applied within the organization.

5. Conduct the testing of patches and non-patch remediation methods on IT devices that use standardized configurations.

6. Oversee the vulnerability remediation process in the organization.

7. Distribute vulnerability and remediation information to local administrators.

8. Perform automated deployment of patches to IT devices using enterprise patch management tools.

9. Configure automatic updates of applications whenever possible and appropriate.

10. Verify vulnerability remediation through network and host vulnerability scanning.

11. Train administrators on how to apply vulnerability remediation.

Use automated patch management tools to expedite the distribution of patches to systems.

Widespread manual patching of computers is becoming ineffective as the number of patches that need to be installed grows and as attackers continue their rapid development of code that exploits vulnerabilities. While patching and vulnerability monitoring may appear to be overwhelming tasks, the use of automated patching technology can make the job less burdensome. Enterprise patch management tools allow the PVG, or a group they work closely with, to automatically distribute updates and patches to many computers quickly. All medium- to large-size organizations should use enterprise patch management tools for most of their computers. Even small organizations should consider migrating to the use of automated patching tools.

Deploy enterprise patch management tools using a phased approach.

Implementing patch management tools in phases allows process and user communication issues to be addressed with a small group before the patch application is deployed throughout the organization. Most organizations should deploy patch management tools first for their standardized desktop systems and single-platform server farms of similarly configured servers. Once this has been accomplished, organizations should address the more difficult issue of integrating multiplatform environments, nonstandard desktop systems, legacy computers, and computers with unusual configurations. Manual methods may be needed for operating systems and applications not supported by automated patching tools, as well as for some computers with unusual configurations, such as embedded systems, industrial control systems, medical devices, and experimental systems. For these systems, there should be a written and implemented procedure for the manual patching process, and the PVG should coordinate the local administrator efforts.

Assess and mitigate the risks associated with deploying enterprise patch management tools.

Enterprise patch management tools, while usually effective at reducing risk, can also create additional security risks for an organization. For example, an attacker could break into the organization's central patch management computer and use the enterprise patch management tool as a way to distribute malicious code efficiently. Organizations should partially mitigate these risks through the application of standard security techniques that should be used when deploying any enterprise-wide application.

Consider using standardized configurations for IT resources.

Organizations will find it much easier and less costly to implement a patch and vulnerability management program when they use standard configurations. Further, the PVG may not be able to test patches adequately if IT devices use nonstandard configurations. Enterprise patch management tools may be ineffective if deployed within an environment where every IT device is configured uniquely, because the side effects of the various patches on the different configurations will be unknown. Comprehensive patch and vulnerability management is almost impossible within large organizations that do not deploy standard configurations.

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.

Organizations should focus their standardization efforts on the systems that make up a significant portion of their IT resources.

Measure the effectiveness of the patch and vulnerability management program in a consistent manner and apply corrective actions as necessary.

An organization can measure its susceptibility to attack, based on the number of patches needed, the number of vulnerabilities identified, and the number of network services running on a per-system basis. These measurements should be taken individually for each computer within the system, and the results then aggregated to determine the system-wide result. A second measure to be made is the mitigation response time, which is based on how quickly an organization can identify, classify, and respond to a new vulnerability and mitigate the potential impact of the vulnerability within the organization. The third measure to be made is the cost of the patch and vulnerability program. This may be difficult to measure because actions are often split between many different personnel and groups. The four main costs that should be taken into consideration are: the PVG, system administrator support, enterprise patch and vulnerability management tools, and incidents that occurred due to failures in the patch and vulnerability management program.

The patch and vulnerability metrics that are taken for a system or IT security program should reflect the patch and vulnerability management maturity level. For example, attack susceptibility metrics such as the number of patches, vulnerabilities, and network services per system are generally more useful for a program with a low maturity level than a high maturity level. Organizations should document what metrics will be taken for each system and the details of each of those metrics. Realistic performance targets for each metric should be communicated to system owners and system security officers. Once these targets have been achieved, more ambitious targets can be set. The level of patch and vulnerability security should be set carefully to avoid overwhelming system security officers and system administrators.

NIST Publications That Support Patch and Vulnerability Management

NIST publications can help you in planning and implementing a comprehensive approach to IT security. For information about the NIST publications that are referenced in the patch and vulnerability management guide, as well as other security-related publications, see http://csrc.nist.gov/publications/index.html.

NIST Special Publication (SP) 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, helps federal agencies develop plans for their IT systems, by documenting their security requirements and describing the controls that are in place or that are planned for meeting those requirements.

NIST SP 800-23, *Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*, helps organizations acquire and use security-related information technology products.

NIST SP 800-26, *Security Self-Assessment Guide for Information Technology Systems*, provides a method for organizations to determine the status of their information security systems and to establish a target for improvement, if needed. The guide defines maturity levels for various aspects of an IT security program.

NIST SP 800-51, *Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme*, describes methods for identifying and organizing known IT system vulnerabilities and provides guidance in the acquisition of CVE-compatible products and services. The CVE is a resource for the IT security community, providing a comprehensive list of publicly known vulnerabilities, an analysis of the authenticity of newly published vulnerabilities, and a unique name for each vulnerability.

NIST SP 800-55, *Security Metrics Guide for Information Technology Systems*, describes the security metrics development and implementation process. Implementation of this process will help demonstrate the adequacy of in-place security controls, policies, and procedures. It also will help justify security control investments and can be used in identifying necessary corrective actions for deficient security controls.

NIST SP 800-61, *Computer Security Incident Handling Guide*, discusses how to organize a security incident response capability and how to handle incidents including denial of service, malicious code, unauthorized access, and inappropriate use of systems.

NIST SP 800-70, *Security Configuration Checklists Program for IT Products—Guidance for Checklists Users and Developers*, provides guidance on creating and using security configuration checklists, which are helpful tools for standardization. NIST SP 800-70 describes the Security Configuration Checklists Program for IT Products, which collects reviewed checklists for a variety of operating systems and applications. Information about the checklists repository is available at http://csrc.nist.gov/checklists/index.html.

Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* (February 2004), establishes security categories for federal information and information systems. The categories are determined based on the potential impact of a loss of confidentiality, integrity, or availability of information or an information system. The security categories should be used to prioritize multi-system vulnerability remediation efforts.

The National Vulnerability Database (NVD) integrates all of the US-CERT vulnerability mitigation products, including vulnerability notes and National Cyber Alert System products. It contains a fine-grained search engine that allows users to search for vulnerabilities containing a variety of characteristics. For example, users can search on product characteristics such as vendor name, product name, and version number, or on vulnerability characteristics such as severity, related exploited range, and type of vulnerability. The NVD provides a vulnerability summary for each CVE vulnerability. Each summary contains attributes of the vulnerability (including a short summary and vulnerable version numbers) and links to advisories, patches, and other resources related to the vulnerability. The NVD is available at http://nvd.nist.gov/.

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