

June 2004

INFORMATION
SECURITY

Continued Action
Needed to Improve
Software Patch
Management



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-04-706](#), a report to congressional requesters

Why GAO Did This Study

Flaws in software code can introduce vulnerabilities that may be exploited to cause significant damage to federal information systems. Such risks continue to grow with the increasing speed, sophistication, and volume of reported attacks, as well as the decreasing period of the time from vulnerability announcement to attempted exploits. The process of applying software patches to fix flaws, referred to as patch management, is a critical process to help secure systems from attacks.

The Chairmen of the House Committee on Government Reform and its Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census requested that GAO assess the (1) reported status of 24 selected agencies in performing effective patch management practices, (2) patch management tools and services available to federal agencies, (3) challenges to performing patch management, and (4) additional steps that can be taken to mitigate the risks created by software vulnerabilities.

What GAO Recommends

GAO recommends that the Director of OMB issue guidance to agencies to provide more refined information on patch management practices, and determine the feasibility of providing selected centralized patch management services. OMB officials generally agreed with our recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-706.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

INFORMATION SECURITY

Continued Actions Needed to Improve Software Patch Management

What GAO Found

Based on agency-reported data, agencies generally are implementing important common practices for effective patch management, such as performing systems inventories and providing information security training. However, they are not consistently performing others, such as risk assessments and testing all patches before deployment. Additional information on key aspects of agencies' patch management practices—such as their documentation of patch management policies and procedures and the frequency with which systems are monitored to ensure that patches are installed—could provide OMB, Congress, and agencies themselves with consistent data that could better enable an assessment of the effectiveness of an agency's patch management processes.

Several automated tools and services are available to assist agencies in performing patch management. These tools and services typically include a wide range of functionality, including methods to inventory computers, identify relevant patches and workarounds, test patches, and report network status information to various levels of management. A centralized resource could provide agencies with selected services such as the testing of patches, a patch management training curriculum, and development of criteria for patch management tools and services. A governmentwide service could lower costs to—and resource requirements of—individual agencies, while facilitating their implementation of selected patch management practices.

Agencies face several challenges to implement effective patch management practices, including (1) quickly installing patches while implementing effective patch management practices, (2) patching heterogeneous systems, (3) ensuring that mobile systems receive the latest patches, (4) avoiding unacceptable downtime when patching high-availability systems, and (5) dedicating sufficient resources toward patch management.

Agency officials and computer security experts identified a number of additional steps that can be taken by vendors, the security community, and the federal government to assist agencies in mitigating the risks created by software vulnerabilities. For example, more rigorous software engineering practices by software vendors could reduce the number of software vulnerabilities and the need for patches. In addition, the research and development of more capable technologies could help secure information systems against cyber attacks. Also, the federal government could use its substantial purchasing power to influence software vendors to deliver more secure systems.

Contents

Letter		1
	Results in Brief	2
	Background	4
	Agencies Are Not Consistently Implementing Common Practices for Effective Patch Management	15
	Automated Tools and Services Can Assist Agencies in Performing Patch Management Activities	22
	Significant Patch Management Challenges Remain	26
	Additional Steps Can Be Taken to Mitigate Risks	30
	Conclusions	35
	Recommendations for Executive Action	36
	Agency Comments	37

Appendixes		
	Appendix I: Objectives, Scope, and Methodology	38
	Appendix II: Staff Acknowledgments	40
	Acknowledgments	40

Table	Table 1: Agencies' Methods of Performing Specific Patch Management Functions	26
--------------	--	----

Figures	Figure 1: Security Vulnerabilities, 1995-2003	5
	Figure 2: Computer Security Incidents, 1995-2003	7

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States General Accounting Office
Washington, D.C. 20548

June 2, 2004

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Adam Putnam
Chairman, Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
Committee on Government Reform
House of Representatives

Federal agencies rely extensively on computerized information systems and their software to carry out their missions. Flaws in software code can introduce vulnerabilities that attackers may attempt to exploit and cause significant damage to federal computer systems. The process of applying software patches to fix flaws, referred to as patch management, is a critical process used to help secure computing systems from attacks.¹

Since 1995, nearly 13,000 security vulnerabilities in software products have been reported. With the increasing sophistication of technology, attacks that once took weeks or months to propagate over the Internet now take only hours or even minutes. While federal agencies can mitigate the risk of cyber attacks by keeping their systems up to date with appropriate patches, applying and maintaining these patches is challenging.

On September 10, 2003, we testified before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census on the role of software patch management in mitigating the risks of cyber incidents.² In that testimony, we stated that patch management is one means to address the increasing vulnerabilities to cybersecurity. You subsequently asked us to assess the (1) reported status of 23 of the agencies under the Chief Financial Officers (CFO) Act of 1990³ and the

¹A patch is a piece of software code that is inserted into a program to temporarily fix a defect. Patches are developed and released by software vendors when vulnerabilities are discovered.

²U.S. General Accounting Office, *Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities*, [GAO-03-1138T](#) (Washington, D.C.: Sept. 10, 2003).

³31 USC Section 901.

Department of Homeland Security (DHS) in performing effective patch management practices, (2) tools and services available to federal agencies to perform patch management, (3) challenges to performing patch management, and (4) additional steps that can be taken to mitigate the risks created by software vulnerabilities.

To address these objectives, we conducted an extensive search of professional information technology (IT) security literature. We also reviewed research studies and reports about cybersecurity-related vulnerabilities to update information provided in our testimony and consulted our prior reports and testimonies on information security. In addition, we interviewed private-sector and federal officials about their patch management experiences, practices, and challenges. Along with these literature searches and interviews, we conducted a Web-based survey of 23 CFO agencies and DHS to determine their patch management practices and reviewed corresponding survey documentation. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that agencies provided to validate their responses. Finally, we met with vendors of commercial software patch management tools and services to discuss and examine their products' functions and capabilities. Appendix I contains a description of our objectives, scope, and methodology. Our work was conducted from September 2003 to May 2004, in accordance with generally accepted government auditing standards.

Results in Brief

Based on agency-reported data, agencies generally are implementing important common patch management-related practices, such as performing systems inventories and providing information security training. However, they are not consistently performing others, such as testing all patches before deployment to help determine whether the patch functions as intended and its potential for adversely affecting an agency's system. Additional information on key aspects of agencies' patch management practices—such as their documentation of patch management policies and procedures and the frequency with which systems are monitored to ensure that patches are installed—could provide the Office of Management and Budget (OMB), Congress, and agencies themselves with consistent data that could better enable an assessment of the effectiveness of an agency's patch management processes.

Several automated tools and services are available to assist agencies in performing patch management. These tools and services typically include a

wide range of functionality, including methods to inventory computers, identify relevant patches and workarounds, test patches, and report network status information to various levels of management. A centralized resource could provide agencies with selected services such as testing patches, developing a patch management training curriculum, and developing criteria for patch management tools and services. Such services could lower costs to—and resource requirements of—individual agencies, while facilitating their implementation of selected patch management practices.

Agencies face several challenges to implementing effective patch management practices, including (1) quickly installing patches while implementing effective patch management practices, (2) patching heterogeneous systems, (3) ensuring that mobile systems receive the latest patches, (4) avoiding unacceptable downtime when patching high-availability systems, and (5) dedicating sufficient resources toward patch management.

Agency officials and computer security experts also identified a number of additional steps that can be taken by vendors, the security community, and the federal government to assist agencies in overcoming challenges. For example, more rigorous software engineering practices by software vendors could reduce the number of software vulnerabilities and the need for patches. In addition, the research and development of more effective technologies could help secure information systems against cyber attacks. Also, the federal government could use its substantial purchasing power to influence software vendors to deliver more security systems.

We are making recommendations to the Director of OMB to provide guidance for agencies to report on key aspects of their patch management practices in their annual Federal Information Security Management Act (FISMA) of 2002 reports, and (2) determine the feasibility of providing selected centralized patch management services to federal civilian agencies, incorporating lessons learned from a now-discontinued service initiated by the Federal Computer Incident Response Center (FedCIRC).⁴ We received oral comments on a draft of our report from officials at OMB's

⁴Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002, P.L. 107-347, December 17, 2002. This act superseded an earlier version of FISMA that was enacted as Title X of the Homeland Security Act of 2002, P.L. 107-296, November 25, 2002.

Office of Information and Regulatory Affairs. These officials generally agreed with our findings and recommendations.

Background

Patch management is a critical process used to help alleviate many of the challenges involved with securing computing systems from attack. A component of configuration management,⁵ it includes acquiring, testing, applying, and monitoring patches to a computer system.

Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. For example, Microsoft Windows 2000 reportedly contains about 35 million lines of code, compared with about 15 million lines for Windows 95. As reported by the National Institute of Standards and Technology (NIST), based on various studies of code inspections, most estimates suggest that there are as many as 20 flaws per thousand lines of software code. While most flaws do not create security vulnerabilities, the potential for these errors reflects the difficulty and complexity involved in delivering trustworthy code.⁶

Security Vulnerabilities and Incidents Are Increasing

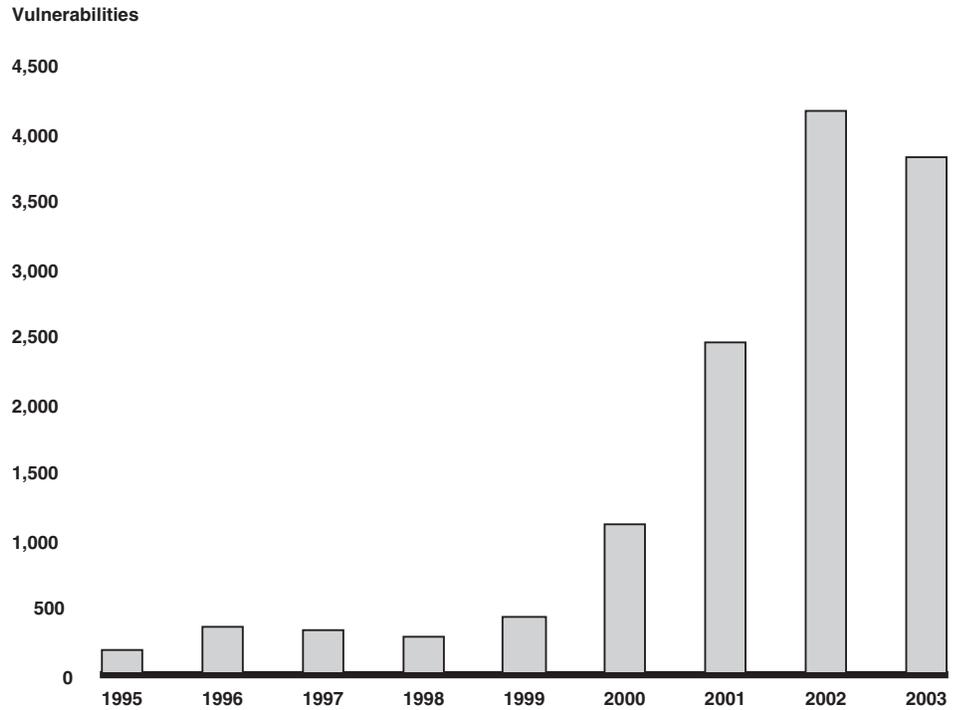
From 1995 through 2003, the CERT[®] Coordination Center (CERT/CC) reported just under 13,000 security vulnerabilities that resulted from software flaws. Figure 1 illustrates the dramatic growth in security vulnerabilities over these years.⁷

⁵Configuration management is the control and documentation of changes made to a system's hardware, software, and documentation throughout the development and operational life of a system.

⁶National Institute for Standards and Technology, *Procedures for Handling Security Patches: Recommendations of the National Institute of Standards and Technology*, NIST Special Publication 800-40 (Gaithersburg, Md.: August 2002).

⁷CERT/CC is a center of Internet security expertise at the Software Engineering Institute, a federally funded research and development center operated by Carnegie-Mellon University.

Figure 1: Security Vulnerabilities, 1995-2003



Source: GAO analysis based on Carnegie-Mellon University's CERT[®] Coordination Center data.

As vulnerabilities are discovered, attackers may attempt to exploit them and can cause significant damage. This damage can range from defacing Web sites to taking control of entire systems and thereby being able to read, modify, or delete sensitive information, destroy systems, disrupt operations, or launch attacks against other organizations' systems. Attacks can be launched against specific targets or widely distributed through viruses and worms.⁸

⁸A virus is a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. In contrast, a worm is an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate.

The sophistication and effectiveness of cyber attacks have steadily advanced. According to security researchers, reverse-engineering patches have become a leading method for exploiting vulnerabilities. Reverse engineering starts by locating the files or code that changed when a patch was installed. Then, by comparing the patched and unpatched versions of those files, a hacker can examine the specific functions that changed, uncover the vulnerability, and exploit it. By using the same tools used by programmers to analyze malicious code and perform vulnerability research, hackers can locate the vulnerable code in unpatched software and build to exploit it.

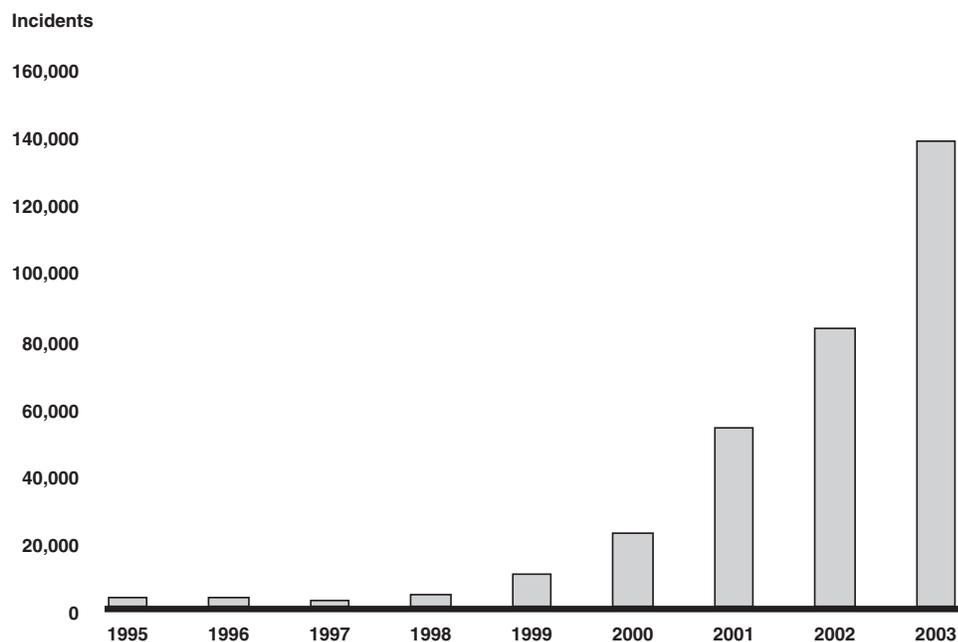
According to NIST, every month skilled hackers post 30 to 40 new attack tools to the Internet for others to download, allowing them to launch attacks. Further, CERT/CC has noted that attacks that once took weeks or months to propagate over the Internet now take just hours, or even minutes. In 2001, security researchers reported that the Code Red worm achieved an infection rate of more than 20,000 systems within 10 minutes, foreshadowing more damaging and devastating attacks. In 2003, the Slammer worm, which successfully attacked at least 75,000 systems, reportedly became the fastest computer worm in history, infecting more than 90 percent of vulnerable systems within 10 minutes. The Witty worm, released on March 19, 2004, reportedly infected as many as 12,000 computers in approximately 45 minutes.

During the last week of February 2004, a spate of new mass e-mail worms were released, and more than half a dozen new viruses were unleashed. The worms were variants of the Bagle and Netsky viruses. The Bagle viruses typically include an infected attachment containing the actual virus, and the most recent versions have protected the infected attachment with a password, which prevents antivirus scanners from examining it. The recent Netsky variants attempt to deactivate two earlier worms and, when executed, reportedly play a loud beeping noise.

The number of computer security incidents within the past decade has risen in tandem with the dramatic growth in vulnerabilities, as the increased number of vulnerabilities provides more opportunities for exploitation. CERT/CC has reported a significant growth in computer security incidents—from about 9,800 in 1999 to over 82,000 in 2002 and to over 137,500 in 2003. And these are only the reported attacks. The director of CERT/CC has estimated that as much as 80 percent of actual security incidents go unreported, in most cases because (1) there were no indications of penetration or attack, (2) the organization was unable to

recognize that its systems had been penetrated, or (3) the organization was reluctant to report the attack. Figure 2 shows the number of incidents reported to the CERT/CC from 1995 through 2003.

Figure 2: Computer Security Incidents, 1995-2003



Source: GAO analysis based on Carnegie-Mellon University's CERT[®] Coordination Center data.

According to CERT/CC, about 95 percent of all network intrusions could be avoided by keeping systems up to date with appropriate patches; however, such patches are often not quickly or correctly applied. Maintaining current patches is becoming more difficult, as the length of time between the awareness of a vulnerability and the introduction of an exploit is shrinking. For example, the Witty worm was released only a day after the announcement of the vulnerability it exploited.

Discovery of Security Vulnerabilities Initiates Response Process

In general, when security vulnerabilities are discovered, a process is initiated to effectively address the situation through appropriate reporting and response—often including the development of a patch.⁹ Typically, this process begins when security vulnerabilities are discovered by software vendors, security research groups, users, or other interested parties, including the hacker community. When a virus or worm is reported that exploits a vulnerability, virus-detection software vendors also participate in the process. When a software vendor is made aware of a vulnerability in its product, the vendor typically first validates that the vulnerability indeed exists. If the vulnerability is deemed critical, the vendor may convene a group of experts, including major clients and key incident-response groups such as FedCIRC and CERT/CC, to discuss and plan remediation and response efforts. In addition, FedCIRC may conduct teleconferences with agency Chief Information Officers (CIO) to coordinate remediation and OMB, through FedCIRC, may request the status of agencies' remediation activities for selected vulnerabilities. After a vulnerability is validated, the software vendor develops and tests a patch or workaround. A workaround may entail blocking access to or disabling vulnerable programs.

Following the development of a patch or workaround, the incident response groups and the vendor typically prepare a detailed public advisory to be released at a set time. The advisory often contains a description of the vulnerability, including its level of criticality; systems that are affected; potential impact if exploited; recommendations for workarounds; and Web site links from which a patch (if publicly available) can be downloaded. Incident-response groups as well as software vendors may continue to issue updates as new information about the vulnerability is discovered.

⁹The Organization for Internet Safety, which consists of leading security researchers and vendors, was formed to standardize the process for handling security vulnerabilities. In July 2003, this organization issued a voluntary framework for vulnerability reporting and response.

Exploited Software Vulnerabilities Can Result in Economic Damage and Disruption of Operations

Although the economic impact of a cyber attack is difficult to measure, a recent Congressional Research Service study cites members of the computer security industry as estimating that worldwide major virus attacks in 2003 cost \$12.5 billion.¹⁰ They further project that economic damage from all forms of digital attacks in 2004 will exceed \$250 billion.

Following are examples of significant damage caused by worms that could have been prevented had the available patches been effectively installed:

- In September 2001 the Nimda worm appeared, reportedly infecting hundreds of thousands of computers around the world, using some of the most significant attack methods of Code Red II and 1999's Melissa virus that allowed it to spread widely in a short amount of time. A patch had been made publicly available the previous month. Reported cost estimates of Nimda range between about \$700 million and \$1.5 billion.
- On January 25, 2003, Slammer reportedly triggered a global Internet slowdown and caused considerable harm through network outages and other unforeseen consequences. As discussed in our April 2003 testimony, the worm reportedly shut down a 911 emergency call center, canceled airline flights, and caused automated teller machine failures.¹¹ According to media reports, First USA Inc., an Internet service provider, experienced network performance problems after an attack by the Slammer worm due to a failure to patch three of its systems. Additionally, the Nuclear Regulatory Commission reported that Slammer also infected a nuclear power plant's network, resulting in the inability of its computers to communicate with each other, disrupting two important systems at the facility. In July 2002, Microsoft had released a patch for its software vulnerability that was exploited by Slammer. Nevertheless, according to media reports, Slammer infected some of Microsoft's own systems. Reported cost estimates of Slammer range between \$1.05 and \$1.25 billion.

¹⁰Congressional Research Service, *The Economic Impact of Cyber Attacks*, (Washington, D.C.: Apr. 1, 2004).

¹¹U.S. General Accounting Office, *Information Security: Progress Made, But Challenges Remain to Protect Federal Systems and the Nation's Critical Infrastructures*, [GAO-03-564T](#) (Washington, D.C.: Apr. 8, 2003).

-
- On August 11, 2003, the Blaster worm was launched to exploit a vulnerability in a number of Microsoft Windows operating systems. When successfully executed, it caused the operating system to fail. Although the security community had received advisories from CERT/CC and other organizations to patch this critical vulnerability, Blaster reportedly infected more than 120,000 unpatched computers in the first 36 hours. By the following day, reports began to state that many users were experiencing slowness and disruptions to their Internet service, such as the need to frequently reboot. The Maryland Motor Vehicle Administration was forced to shut down, and systems in both national and international arenas were also affected. Experts consider Blaster, which affected a range of systems, to be one of the worst exploits of 2003. Microsoft reported that at least 8 million Windows computers have been infected by the Blaster worm since last August.
 - On May 1 of this year, a new worm, referred to as Sasser, was reported, which exploits a vulnerability in the Windows Local Security Authority Subsystem Service component. This worm can compromise systems by allowing a remote attacker to execute arbitrary code with system privileges. According to the United States Computer Emergency Readiness Team (US-CERT), systems infected by this worm may suffer significant performance degradation. Sasser, like last year's Blaster, exploits a recent vulnerability in a component of Windows by scanning for vulnerable systems. Estimates by Internet Security Systems, Inc. place the Sasser infections at 500,000 to 1 million machines. Microsoft has reported that 9.5 million patches for the vulnerability were downloaded from its Web site in just 5 days.

Federal Efforts to Address Software Vulnerabilities

The federal government has taken several steps to address security vulnerabilities that affect agency systems, including efforts to improve patch management. Specific actions include (1) requiring agencies to annually report on their patch management practices as part of their implementation of FISMA, (2) identifying vulnerability remediation as a critical area of focus in the President's National Strategy to Secure Cyberspace, and (3) creating US-CERT.

FISMA permanently authorized and strengthened the information security program, evaluation, and reporting requirements established for federal agencies in prior legislation.¹² In accordance with OMB's reporting instructions for FISMA implementation, maintaining up-to-date patches is part of FISMA's system configuration management requirements. The 2003 FISMA reporting instructions that specifically address patch management practices include agencies' status on (1) developing an inventory of major IT systems, (2) confirming that patches have been tested and installed in a timely manner, (3) subscribing to a now-discontinued governmentwide patch notification service, and (4) addressing patching of security vulnerabilities in configuration requirements.

The President's National Strategy to Secure Cyberspace was issued on February 14, 2003, to identify priorities, actions, and responsibilities for the federal government as well as for state and local governments and the private sector, with specific recommendations for action to DHS. This strategy identifies the reduction and remediation of software vulnerabilities as a critical area of focus. Specifically, the strategy identifies the need for

- a better-defined approach on disclosing vulnerabilities, to reduce their usefulness to hackers in launching an attack;
- creating common test beds for applications widely used among federal agencies; and
- establishing best practices for vulnerability remediation in areas such as training, use of automated tools, and patch management implementation processes.

In June 2003 DHS created the National Cyber Security Division (NCSD) to build upon the existing capabilities transferred to DHS from the former Critical Infrastructure Assurance Office, the National Infrastructure Protection Center, FedCIRC, and the National Communications System. The mission of NCSD includes patch management-related activities, among them analyzing cyber vulnerabilities and coordinating incident response. Last September, DHS's NCSD—in conjunction with CERT/CC and the private sector—established a new service, US-CERT, as the center for

¹²Title X, Subtitle G—Government Information Security Reform, *Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*, P.L. 106-398, October 30, 2000.

coordinating computer security preparedness and response to cyber attacks and incidents. Specifically, US-CERT is intended to aggregate and disseminate cybersecurity information to improve warning and response to incidents, increase coordination of response information, reduce vulnerabilities, and enhance prevention and protection. This free service—which includes notification of software vulnerabilities and sources for applicable patches—is available to the public, including home users and both government and nongovernment entities.

US-CERT also provides a service through its National Cyber Alert System to identify, analyze, prioritize, and disseminate information on emerging vulnerabilities and threats. This alert system was designed to provide subscribers with reliable, timely, and actionable information via e-mail by issuing security alerts, tips, and bulletins containing information on vulnerabilities, exploits, and available patches or workarounds. It also provides computer security best practice tips, including a discussion of software patches. This free service is available to all.

Agencies Can Utilize Other Resources to Mitigate Vulnerabilities

In addition to vulnerability analysis and reporting centers such as US-CERT and CERT/CC, a variety of other resources are also available to provide information related to vulnerabilities and their exploits. NIST's Special Publication 800-40, *Procedures for Handling Security Patches*, provides a systematic approach for identifying and installing necessary patches or mitigating the risk of a vulnerability, including steps such as creating and implementing a patch process, identifying vulnerabilities and applicable patches, and patching procedures, among others.¹³ Another resource is NIST's ICAT, which offers a searchable index leading users to vulnerability resources and patch information. ICAT links users to publicly available vulnerability databases and patch sites, thus enabling them to find and fix vulnerabilities existing on their systems. It is based on common vulnerabilities and exposures (commonly referred to as CVE) naming standards. These are standardized names for vulnerabilities and other information security exposures, compiled in an effort to make it easier to share data across separate vulnerability databases and tools. CVE compatibility is increasingly being incorporated into various security products.

¹³NIST Special Publication 800-40.

In addition, a variety of Internet mailing lists provides a database of vulnerabilities and serves as a forum for announcing and discussing vulnerabilities, including information on how to fix them. For example, one vendor-provided list monitors thousands of products to maintain a vulnerability database and also provides security alerts. The SysAdmin, Audit, Network, Security (SANS) Institute maintains lists of the top 20 most critical Internet security vulnerabilities, commonly known as the SANS Top Twenty, which includes step-by-step instructions and references to additional information on how to remediate vulnerabilities.¹⁴

In March of this year, the Open Source Vulnerability Database (OSVDB)—a vendor-neutral database operated by security industry volunteers and supported by Digital Defense, Inc., and Winterforce—was made available at no cost to the public.¹⁵ This database aims to be a comprehensive, single source for providing detailed, current, and accurate information for all known vulnerabilities. As of June 1, this database contained information on about 3,000 reported and reviewed vulnerabilities.

In addition, vendors such as Microsoft and Cisco provide software updates on their products, including notices of known vulnerabilities and their corresponding patches; they also provide software options for automatically downloading and installing patches. Finally, vendors of patch management tools and services, discussed later, offer central databases of the latest patches, incidents, and methods for mitigating risks before a patch can be deployed or has been released.

¹⁴The SANS Institute is a cooperative research and education organization comprising security practitioners in government agencies, corporations, and universities around the world. SANS develops, maintains, and makes available a large collection of research documents about various aspects of information security, and operates the Internet's early warning system, the Internet Storm Center.

¹⁵Digital Defense, Inc., provides the server and bandwidth for OSVDB and has also contributed the development of the software for this project. Winterforce is providing OSVDB with extensive documentation support, as well as consulting services, to help ensure that the goals of OSVDB are properly communicated and achieved.

Collaborative Response to Two Software Vulnerabilities

According to FedCIRC officials, the federal government has on occasion taken additional steps to assist agencies in mitigating known vulnerabilities through patch management. Such steps include issuing security advisories, issuing data calls to obtain status information on agencies' patching efforts, and initiating teleconferences with vendors. As discussed in our September 2003 testimony, the following are examples of the collaborative efforts by the federal government and private sector security community to respond through patch management to the threat of potential attacks for two critical vulnerabilities identified last July: Cisco's Internet Operation System and Microsoft's Windows Distributed Component Object Model Remote Procedure Call.¹⁶

Cisco Systems, Inc., which controls about 82 percent of the worldwide share of the Internet router¹⁷ market, discovered a critical vulnerability in its IOS software that could allow an intruder to effectively shut down unpatched routers, blocking network traffic. Cisco had informed the federal government of the vulnerability prior to public disclosure and worked with different security organizations and government organizations to encourage prompt patching. Specifically, on July 16, Cisco issued a security bulletin to publicly announce the critical vulnerability in its IOS software and provide workaround instructions and a patch. In addition, FedCIRC issued advisories to federal agencies and DHS advised private-sector entities of the vulnerability. Over the next 2 days, OMB requested that federal agencies report to CERT/CC on the status of their actions to patch the vulnerability, and DHS issued an advisory update in response to an exploit that was posted online. That same week, FedCIRC, OMB, and DHS's NCSA held a number of teleconferences with representatives from the executive branch.

¹⁶Distributed Component Object Model (DCOM) allows direct communication over the network between software components. Remote Procedure Call (RPC) is a protocol of the Windows operating system that allows a program from one computer to request a service from a program on another computer in a network, thereby facilitating interoperability.

¹⁷Routers are hardware devices or software programs that forward Internet and network traffic between networks and are critical to their operation.

The federal government also worked collaboratively with Microsoft when the Blaster worm was launched last summer. The federal government's response to this vulnerability included coordination with the private sector to mitigate the effects of the worm.¹⁸ FedCIRC issued the first advisory to encourage federal agencies to patch the vulnerability, followed by several similar advisories from DHS. The following week, DHS issued its first advisory to heighten public awareness of the potential impact of an exploit of this vulnerability. Four days later, on behalf of OMB, FedCIRC requested that federal agencies report on the status of their actions to patch the vulnerability. NCSA also hosted several teleconferences with federal agencies, CERT/CC, and Microsoft.

Agencies Are Not Consistently Implementing Common Practices for Effective Patch Management

Common patch management practices—such as establishing and enforcing standardized patch management policies and procedures and developing and maintaining a current technology inventory—can help agencies establish an effective patch management program and, more generally, assist in improving an agency's overall security posture. Survey results show that the 24 agencies are implementing some common practices for effective patch management. Specifically, all report that they have some level of senior executive involvement in the patch management process, perform a systems inventory, and provide information security training. However, agencies face a number of patch management challenges—as discussed later—and are inconsistent in their development of patch management policies and procedures, patch testing, systems monitoring, and performance of risk assessments. Without consistent implementation of patch management practices, agencies are at increased risk to attacks that exploit software vulnerabilities in their systems. Information on key aspects of agencies' patch management practices could provide data that could better enable an assessment of the effectiveness of an agency's patch management processes.

Common Practices for Effective Patch Management Have Been Identified

In our September 2003 testimony, we discussed common practices for effective patch management identified in security-related literature from several groups, including NIST, Microsoft, patch management software vendors, and other computer security experts. Common elements of effective patch management identified by these groups include

¹⁸See [GAO-03-1138T](#) for a detailed chronology of events.

-
- centralized patch management support,
 - senior executive support,
 - standardized patch management policies and procedures,
 - training,
 - current technology inventory,
 - risk assessment,
 - testing, and
 - monitoring through network and host vulnerability scanning.¹⁹

Agencies' Degree of Centralization Varies

NIST guidance advocates creating a centralized group in charge of handling patches and vulnerabilities that support the patching efforts of local system administrators. A systematic, comprehensive, and documented patching process can improve an agency's ability to respond to the large number of software patches.

Agencies' centralization of common practices for effective patch management varies. While some agencies centralize their patch management processes, others use a decentralized approach, and still others a combination of both approaches. For example, the responsibility for distributing and notifying the agency's component levels of critical patches can be centralized, while the responsibility for testing and applying patches to specific systems may be decentralized to reside at the component level. Specifically, of the 24 agencies surveyed, 7 report using a centralized approach, 8 are decentralized, and 9 use a combination of both.

¹⁹The common patch management practices of receiving notification of relevant vulnerabilities and distributing critical patches are discussed in the subsequent section on automated tools and services.

Agencies' Senior Executives Are Involved in Patch Management Efforts

Management's recognition of information security risk and its interest in taking steps to manage and understand risks is important to successfully implementing any information security-related process. Additionally, ensuring that appropriate resources are applied and that appropriate patches are deployed is important. FISMA establishes information security roles and responsibilities for certain agency executives, including the agency head, CIO, and senior agency information security officer, sometimes called the chief information security officer (CISO). Under FISMA, the agency head is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access to, use, disclosure, disruption, modification, or destruction of information. FISMA further states that the agency head shall delegate to the CIO the authority to ensure compliance with its requirements and develop and maintain an agencywide information security program, security policies, procedures, and control techniques. Additionally, the CIO is responsible for designating a senior agency information security officer or CISO. This CISO must possess appropriate professional qualifications to administer the functions described in FISMA, have information security duties as the primary duty, and head an office with the mission and resources to assist in ensuring agency compliance with FISMA.

All 24 agencies indicated that the CISO is the individual most involved in patch management activities. Specifically, the CISO is involved in managing risk, ensuring that appropriate resources are dedicated, training computer security staff, complying with policies and procedures, and monitoring the status of patching activities. Agencies reported that the CIO also has a significant level of involvement in these activities. Further, most agencies reported that their agency head was involved in patch management efforts to some degree.

Some Agencies Have Not Developed Patch Management Policies or Procedures

Standardized policies and procedures are necessary for effective patch management. Typical policies include elements such as assigning roles and responsibilities, performing risk assessments, and testing patches. Procedures outline the specific steps for carrying out these policies. Without standardized policies and procedures, patch management can be an ad-hoc process—potentially allowing each subgroup within an entity to implement patch management inconsistently or not at all.

Survey results indicate that not all agencies have established patch management policies and procedures. Two-thirds (16 of 24) report having agencywide patch management policies, while 8 have no policies. Regarding patch management procedures, 14 of the 24 agencies reported affirmatively, while 10 do not have procedures in place.

Agencies Are Providing Information Security Training

FISMA requires agencies to provide security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of information security risks associated with their activities, and of their responsibilities in complying with agency policies and procedures designed to reduce these risks. In addition, agencies are required to provide training on information security to personnel with significant security responsibilities. Further, NIST recommends that individuals involved in patch management have the skills and knowledge needed to perform their responsibilities and that system administrators be trained in identifying new patches and vulnerabilities.

Most of the 24 agencies reported that they provide both on-the-job and classroom training in computer security, including patch management, to system owners, administrators, and IT security staff. Survey results also indicated that some of the 24 agencies are providing security awareness training, as well as developing Web-based training curricula.

Agencies Are Developing and Maintaining System Inventories

A complete and updated inventory assists agencies in determining the number of systems that are vulnerable and require remediation, as well as in locating the systems and identifying their owners. FISMA requires that the head of each agency maintain and develop an inventory of major information systems. Further, NIST's Special Publication 800-40, *Procedures for Handling Security Patches*, identifies a systems inventory requirement as a key priority for effective patch management. Without a complete inventory, it is more difficult to implement effective agencywide patch management and maintaining current patches can be riskier, less consistent, and more expensive.

In our September 2003 testimony, we reported that an important element of patch management is the creation and maintenance of a current inventory of hardware equipment, software packages, services, and other technologies installed and used by an organization. We noted that in their 2003 FISMA reports, 13 agencies reported that an inventory of major

systems was developed, and 6 reported that the development was in progress. Agencies' inspectors general also assessed the status of agency efforts to develop an inventory of major IT systems. Their FISMA reports indicated that only 8 had developed an inventory and 9 agencies had started—but not yet completed—one.

All 24 agencies reported that they develop and maintain an inventory of major information systems as required by FISMA. Agencies do so by using a manual process, an automated tool, or an automated service. The majority of agencies maintain this inventory at both the agencywide and component level. Specifically, 9 of the 24 agencies maintain their inventories at the agencywide level only, 14 maintain their inventories at both levels, and 1 agency at the component level only.

Agencies Are Not Consistently Performing Risk Assessments

Risk is the negative impact of a vulnerability's being exploited, considering both the probability and the impact of occurrence. A risk assessment can be used to determine the extent of the potential threat and the risk associated with it. Performing a patch-focused risk assessment evaluates each system for threats, vulnerabilities, and the criticality of a system to an agency's mission. It can also measure the level of risk associated with the adverse impact resulting from a vulnerability being exploited. By not performing a risk assessment, agencies may deploy patches that disrupt critical systems or applications that support an agency's operations.

When a vulnerability is discovered and a related patch and/or alternative workaround is released, the agency should consider the importance of the vulnerable system to operations, the criticality of the vulnerability, and the risk of applying the patch. Because some patches can cause unexpected disruption to agencies' systems, organizations may choose not to apply every patch. NIST recommends that a risk assessment be performed to determine the prioritization of the systems to be patched.

Just under half of the 24 agencies said they perform a documented risk assessment of all major systems to determine whether to apply a patch or an alternative workaround. Agencies that do not perform a documented risk assessment reported that they consider which patches to deploy based on factors such as the risk of deploying the patch, the level of system criticality to agency operations, the level of criticality of the vulnerability, or other criteria, such as the adverse impact on applications.

Most Agencies Are Not Testing All Patches Before Deployment

Another critical step is to test each patch against the various agency system configurations in a test environment to determine any impact on the network before deploying the patch to the affected systems. Patches can easily produce unintended consequences; a patch may change the system behavior such that it causes other programs to crash or otherwise fail. For instance, certain security patches have been recalled—as recently as April of this year—because they caused systems to fail or are too large for a computer’s capacity. Other examples of unintended consequences include patches that force other applications to shut down and patches that undo the effects of previously applied patches. Predeployment testing helps determine whether the patch functions as intended and its potential for adversely affecting the agency’s systems.

In addition to identifying the potential for unintended consequences, the testing of patches can ensure that agencies have addressed the vulnerability as intended. Testing may also identify other critical vulnerabilities not made public by vendors. For example, one federal agency’s testing revealed that a vendor’s patch notification did not identify vulnerabilities in the underlying operating system. The agency’s testing results prompted an advisory informing all federal agencies to patch all machines using that operating system.

Survey results showed that although all 24 agencies test some patches against their various systems configurations before deployment, only 10 agencies reported testing all patches, 11 test more than half but not all patches, 2 test half or fewer, and 1 agency did not know. While all surveyed agencies reported that they test patches to some extent, most agencies do not have testing policies in place. Survey results show that only 7 agencies have testing policies for all patches, and 2 have policies for only testing critical patches. The remaining 15 agencies reported that they do not have any testing policies in place. Agencies indicated several reasons for not testing all patches, including a determination that the urgency or criticality of a vulnerability required immediate patching and that a patch was anticipated to have a minimal impact on their systems. Some agencies also stated that in most cases they do not test patches issued routinely by Microsoft.

Agencies Do Not Regularly Monitor the Status of Deployed Patches

In addition to testing, it is important to regularly monitor the status of patches once they are deployed. Networks can be scanned on a regular basis to assess the network environment and determine whether patches

have been effectively applied. By doing so, agencies can ensure that patches are installed correctly and can help maintain a stable computing environment and determine the integrity of a patch. In addition, monitoring helps ensure that a patched system continues to be in compliance with the agency's network configuration requirements.

Survey results show that most agencies do not regularly monitor all systems. Only 4 agencies indicated that they monitor all of their systems on a regular basis. However, the remaining agencies surveyed indicated that they perform some monitoring activities. All 24 agencies reported scanning networks and hosts to oversee the deployment of patches and noted that the extent to which systems are monitored and the frequency with which they are monitored varies.

Agencies indicated that the frequency of system monitoring is based on two factors— (1) the criticality of the vulnerability and (2) the criticality of the computer system. Five agencies stated that they monitor based on the criticality of the vulnerability; 14 reported that the frequency depends on both the criticality of the vulnerability and the criticality of the computer system. Five agencies indicated that the frequency of monitoring does not vary based on either of these factors.

More Refined FISMA Information Could Assist Management Oversight

Although OMB and federal agencies recognize that implementing common practices for effective patch management can help agencies mitigate the risk of attack and improve their overall security posture, the results of our survey indicate that agencies are not consistently performing these common practices. More refined information on key aspects of agencies' patch management practices—such as their documentation of patch management policies and procedures, their testing of new patches in their specific computing environments prior to installation, and the frequency with which systems are monitored to ensure that patches are installed— could provide OMB, Congress, and agencies themselves with data that could better enable an assessment of the effectiveness of an agency's patch management processes.

Automated Tools and Services Can Assist Agencies in Performing Patch Management Activities

Several automated tools and services are available to assist agencies with patch management. A patch management tool is an application that automates a patch management function, such as scanning a network and deploying patches. Patch management services are third-party resources that provide services such as notification, consulting, and vulnerability scanning. Tools and services can make the patch management process more efficient by automating otherwise time-consuming tasks, such as manually keeping up with the continuous flow of new patches.

Patch management tools can be either scanner-based (nonagent) or agent-based. Scanner-based tools can scan a network, check for missing patches, and allow a system administrator to patch multiple computers. These tools are well suited for smaller organizations due to their inability to serve a large number of users without breaking down or requiring major changes in procedure. Agent-based products place small programs, or agents, on each computer, to periodically poll a patch database—a server on the network—for new updates, giving the system administrator the option of applying the patch. Agent-based products require up-front work to integrate agents into the workstations and in the server deployment process, but are better suited to large organizations due to their ability to generate less network traffic and provide a real-time network view. Finally, some patch management tools are hybrids—allowing the user to utilize agents or not. Agencies can also contract with third parties to develop and maintain their patch management processes.

Commercially available tools and services typically include, among others, methods to

- inventory computers and the software applications and patches installed;
- identify relevant patches and workarounds and gather them in one location;
- group systems by departments, machine types, or other logical divisions;
- manage patch deployment;
- scan a network to determine the status of patches and other corrections made to network machines (hosts and/or clients);

-
- assess machines against set criteria, including required system configurations;
 - access a database of patches;
 - test patches; and
 - report information to various levels of management about the status of the network.

FedCIRC Provided Agencies with Centralized Federal Patch Notification Service

In our September 2003 testimony, we reported on FedCIRC's Patch Authentication and Dissemination Capability (PADC), a service initiated in February 2003 to provide users with a method of obtaining information on security patches relevant to their enterprise and access to patches that had been tested in a laboratory environment. This service was offered to federal civilian agencies at no cost. Twenty of the 24 agencies we surveyed reported that they had subscribed to the service.

Subscribers obtained an account license that allowed them to receive notifications and log into the secure Web site to download patches. They received notification of threats, vulnerabilities, and the availability of patches on the basis of profiles they had created that defined the technologies they used. They were notified by e-mail or pager message when a vulnerability or patch that affected one or all of their systems had been posted to the secure Web site.

Last year, OMB reported that while many agencies had established PADC accounts, actual usage of those accounts was extremely low. A FedCIRC official also stated that there was a general lack of interest from agencies in using PADC, and that although agencies were provided with access to the tool, they did not activate available accounts. Many agencies only used the service as a tool to obtain notification of patches—a service that is provided at no cost from vendors such as Microsoft.

In an effort to improve the implementation and usefulness of PADC, FedCIRC officials held meetings with contractor and user groups, visited agencies, and provided Web-based training. Interest in improving the service was expressed. For example, one of the surveyed agencies' officials stated that PADC could improve its value by establishing an independent patch test laboratory, which could then advise agencies of test results and

provide recommendations. However, officials indicated that such upgraded services would incur significant costs.

According to agency officials, there were limitations to the PADC service. Although free to agencies, only about 2,000 licenses or accounts were available because of monetary constraints. According to FedCIRC officials, this constraint required them to work closely with participating agencies to balance the number of licenses that a single agency required with the need to allow multiple agencies to participate. For example, the National Aeronautics and Space Administration initially requested more than 3,000 licenses—one for each system administrator. Other limitations of the service cited by the agencies include that it did not support all platforms or technologies within an agency, that notification of patches was not timely, and that the level of services provided was minimal.

According to FedCIRC officials, PADC was terminated on February 21, 2004, because of low levels of usage, the cost to upgrade services, and negative agency feedback on the usefulness of the service. They also noted that there are no immediate plans for another contractual service. However, discussions with federal agencies on addressing patch management issues remain ongoing through the recently formed Chief Information Security Officers forum, sponsored by DHS.

In the absence of PADC, agencies are left to independently perform all components of effective patch management, including functions that may be common across the federal government. A centralized resource that incorporates lessons learned from PADC's limitations could provide standardized services, such as the testing of patches, a patch management training curriculum, and development of criteria for patch management tools and services. In fact, a FedCIRC official stated that the organization is considering providing agencies with a clearinghouse of information on commercially available patch management tools and services. A governmentwide service could lower costs to—and resource requirements of—individual agencies, while facilitating their implementation of selected patch management practices.

Other Automated Patch Management Methods Are Available

In addition to resources discussed earlier, such as vulnerability databases and analysis and warning centers, agencies can use other tools and methods to assist in their patch management activities. For example, they can maintain a database of the versions and latest patches for each server and each client in their network and track the security alerts and patches

manually. This method is, however, labor-intensive. Agencies can also employ systems management tools with patch-updating capabilities to deploy the patches. This method requires that agencies monitor for the latest security alerts and patches. One agency reported that it developed a program in house to download patches, upgrades, and antivirus files, while another agency reported that it created a tool to apply settings and vendor patches, validate and maintain compliance, and report system status. One agency indicated that it uses the maintenance contract with its vendors to receive notification of applicable vulnerabilities.

Further, software vendors may provide automated tools with customized features to alert system administrators and users of the need to patch and, if desired, to automatically apply patches. For example, Microsoft currently provides Software Update Services, a free service for automating the downloading and deployment of patches. Several agencies indicated that they subscribe to this service for tasks such as receiving notification of known vulnerabilities and obtaining and deploying patches.

Agencies Utilize Automated Patch Management Tools and Services

Survey results show that such tools and services play a large part in the patching practices of federal agencies. Twenty-three of 24 agencies use commercially available patch management tools. Twenty of 24 agencies use commercially available services, 3 do not, and 1 agency did not know the status of services used there. Table 1 summarizes agencies' methods of performing specific patch management functions as reported by the 24 agencies.

Table 1: Agencies' Methods of Performing Specific Patch Management Functions

Function	Only performed manually	Only performed using automated tools or services	Performed using both automated and manual methods	Neither
Develop and maintain the inventory of major information systems as required by FISMA	10	2	12	0
Scan networks and hosts to identify known vulnerabilities	0	8	16	0
Receive notification of a vulnerability	2	3	19	0
Identify the relevant patch and/or workaround, if a patch is not yet available, for the affected system(s)	1	3	20	0
Obtain the available patch from the vendor or other trusted source	1	3	20	0
Test patches against specific systems' configurations before deployment	15	0	9	0
Distribute patches to system administrators	2	2	19	1
Deploy patches to all affected systems	0	2	22	0
Scan networks and hosts to monitor (i.e., oversee) that patches have been deployed	0	8	16	0
Verify that remote users of managed systems, who were not connected to the network when the patch was distributed, have received and deployed patches	3	6	12	1 ^a
Report the status of vulnerability remediation to management	11	1	12	0

Source: GAO analysis of agency-provided survey data.

^aTwo agencies did not know how this process was performed, if at all.

Significant Patch Management Challenges Remain

According to security experts and agency officials, the federal government faces several challenges to implementing effective patch management practices. Our work identified several additional steps that can be taken to address the risks associated with software vulnerabilities.

Agencies face a number of common patch management obstacles, including (1) quickly installing patches while implementing effective patch management practices, (2) patching heterogeneous systems, (3) ensuring that mobile systems receive the latest patches, (4) avoiding unacceptable downtime when patching high-availability systems, and (5) dedicating sufficient resources toward patch management.

High Volume and Increasing Frequency of Patches Limits Effective Patch Management Implementation

Several of the agencies we surveyed indicated that the sheer quantity and frequency of needed patches posed a challenge to the implementation of the recommended patch management practices—including performing patch-based risk assessments and testing patches to ensure against any adverse effects.

Timely patching is critical to maintaining the operational availability, confidentiality, and integrity of agencies' IT systems. As increasingly virulent computer worms have demonstrated, agencies need to keep systems updated with the latest security patches. However, security experts have noted that malicious code writers have shortened the length of time between disclosure of a vulnerability and the release of an exploit to just a few days. As previously discussed, the Witty worm began to spread the day after the applications' vulnerability was publicized and has been reported to represent the shortest interval between vulnerability disclosure and worm release. Due to the devastating consequences of an attacker's exploiting an unpatched vulnerability, agencies are pressured to install patches as quickly as they are received.

The urgency in patching a security vulnerability can limit or delay implementation of common practices for effective patch management. For example, NIST has noted that there is at best minimal time (hours to days) to test patches before implementing them, because attacks attempting to exploit these vulnerabilities are likely to occur as soon as the vulnerability is discovered or publicized. Testing of patches requires significant time; according to CERT/CC, some financial institutions require 6 weeks of regression testing before a patch is deployed. In addition, third-party vendors often take months after a patch is released to certify that installing it will not break their systems.

Heterogeneity of Systems Complicates Patching

In response to our survey, several agencies indicated that the heterogeneity of their systems—variations in platforms, configurations, and deployed applications—complicates their patching processes. Agencies noted that their mixture of legacy systems and commercial-off-the-shelf applications has led to instances in which patches were not applied to all computers due to concerns over their impact on operations. Further, their unique IT infrastructures can make it challenging for agencies to determine which systems are affected by a software vulnerability. For example, it was widely reported that the Slammer worm exploited a vulnerability found in two specific Microsoft SQL Server database applications. However, because those 2 vulnerable applications are utilized in more than 25 of Microsoft's other database and desktop applications—and reportedly in about 130 third-party applications, agencies could not easily determine which applications were affected on their networks.²⁰

Mobile Systems May Not Receive Current Patches

Several agencies reported challenges in ensuring that their mobile computers—such as laptops, digital tablets, and personal digital assistants—receive the most current patches as soon as users connect to the network. Mobile computers can be used at physical locations outside an agency's defined network security perimeter. Consequently, they may not be on the network at the right time to receive appropriate patches that an agency deploys and are at significant risk of not being patched. For example, one private-sector entity stated that its network first became affected by the Microsoft RPC vulnerability when remote users plugged their laptops into the network after being exposed to the vulnerability from other sources. Also, users of mobile systems may utilize a remote connection to download the patch file. Depending on the size of the package to be distributed and the bandwidth available to the machine, patches may be improperly downloaded and installed. When users then physically connect their mobile computers to the agency network, they may introduce a vulnerable system into the network. However, tools are available to automatically scan and patch mobile systems when they connect to an agency's network.

²⁰Slammer exploited a vulnerability in Microsoft's SQL Server 2000 database and the Microsoft SQL Server 2000 Data Engine (MSDE 2000) software. Office XP, Small Business Manager, Visual Studio, and Host Integration Server are some of the 27 Microsoft products that utilize MSDE 2000.

Patching High-Availability Systems Causes Unacceptable Downtime

Some critical systems are required to be continuously available, and an agency's ability to fulfill its mission could be significantly affected by the downtime required to install patches. Reacting to new security patches as they are introduced can interrupt normal and planned IT activities, and any downtime incurred during the patching cycle interferes with business continuity. When redundant systems are used, patches can be alternately applied to each system. However, redundant systems may not be technologically or economically feasible.

For example, critical high-availability systems include control systems, commercial satellite systems, and certain financial systems. Control systems are computer-based systems that are used within many of our nation's infrastructures and industries to monitor and control sensitive processes and physical functions.²¹ These systems are increasingly based on standardized technologies that are vulnerable to cyber attack. However, because they can be used to perform complex functions, like managing most activities in a municipal water system or even a nuclear power plant, they have high-availability requirements. Frequent downtime is also considered unacceptable for commercial satellite systems, which are also vulnerable to cyber attack.²² Federal contracts with commercial satellite service providers specify high availability and reliability levels to emphasize the importance of continuous service.²³ Certain financial systems are also required to be continuously available, such as the Fedwire funds transfer system that routes and settles Federal Reserve Banks' payment orders. The Fedwire system is expected to be available 99.85 percent of the time and therefore cannot easily be taken off line to install

²¹For our report on the cybersecurity of control systems, see U.S. General Accounting Office, *Critical Infrastructure Protection: Challenges and Efforts to Control Systems*, [GAO-04-354](#) (Washington, D.C.: Mar. 15, 2004).

²²For our report on the security of satellite systems, see U.S. General Accounting Office, *Critical Infrastructure Protection: Commercial Satellite Security Should Be More Fully Addressed*, [GAO-02-781](#) (Washington, D.C.: Aug. 30, 2002).

²³When used in reference to satellite systems, *availability* is the ratio of the total time a service is being used during a given interval to the length of the interval. For example, a service provider may state that its services will be available 99.99 percent of the time over a year, which amounts to 53 minutes of accumulated outages for all causes over the course of the year. Reliability is the probability that a service will perform its required function for a specified period of time under stated conditions. Federal Telecommunications Standards Committee, *Telecom Glossary 2000* (Feb. 2, 2001).

patches. For example, a Fedwire system outage that lasts 2 minutes is considered by the Federal Reserve to be a “major outage.”

Agencies Face Challenges in Dedicating Sufficient Resources to Patch Management Practices

Thirteen of the 24 agencies that responded to our survey indicated that dedicating sufficient resources was a significant challenge they faced in implementing an effective patch management process. Despite the growing market of patch management tools and services that can track machines that need patches and automate patch downloads from vendor sites, agencies noted that effective patch management is a time-consuming process that requires dedicated staff to assess vulnerabilities and test and deploy patches. Further, once a patch is deployed, additional efforts are required to ensure that all vulnerable computers have been effectively fixed. Agencies recognized the need to devote time and funding to the patch management process, as well as to the training of skilled system administrators. For this reason, they may benefit from a shared patch management resource that provides centralized and dedicated functions such as testing and training.

Additional Steps Can Be Taken to Mitigate Risks

We identified a number of steps that can be taken to address the risk associated with software vulnerabilities and patch management challenges, including (1) reducing the number of potential vulnerabilities through better software engineering, (2) incorporating a defense-in-depth strategy into agencies’ IT infrastructures, (3) improving currently available tools, (4) researching and developing new security technologies, and (5) leveraging the federal government’s buying power to demand more secure products. DHS has begun efforts to implement additional steps through the establishment of collaborative task forces.

Better Software Engineering Can Reduce Vulnerabilities

More rigorous engineering practices, which include a formal development process, developer training on secure coding practice, and code reviews, can be employed when designing, implementing, and testing software products to reduce the number of potential vulnerabilities and thus minimize the need for patching. It is much less costly and more secure to identify defects during software development than to patch vulnerabilities after the product has been distributed.

However, CERT/CC has reported that because software developers do not devote enough effort to applying lessons learned about the causes of vulnerabilities, the same types of vulnerabilities identified in earlier versions continue to appear in newer versions of products. Buffer overflows, for example, which may allow an attacker to gain control of a machine or mount a denial of service attack, represent a significant proportion of all overall software security vulnerabilities.²⁴ For example, the Blaster and Sasser worms both exploited buffer overflow vulnerabilities in Microsoft products.

Vendors that are proactive and adopt known effective software engineering practices can drastically reduce the number of flaws in their software products. For example, as part of its Trustworthy Computing Initiative, Microsoft is planning to undertake several steps to strengthen the software development process. According to Microsoft officials, creating secure software starts with a formal design process that verifies the security properties of the software at each well-defined stage of construction. The need to consider security “from the ground up” is a fundamental tenet of secure systems development. Such a process is intended to minimize the number of security vulnerabilities injected into the design, code, and documentation in the first place and to detect and remove those vulnerabilities as early in the development life cycle as possible. From inception to release, a development team, along with a central security team, makes plans to evaluate the security of the software.

Implementing “Defense-in-Depth” Can Reduce Vulnerabilities

According to security experts, a best practice for protecting systems against cyber attacks is for agencies to build successive layers of defense mechanisms at strategic points in their IT infrastructures. This approach, commonly referred to as *defense-in-depth*, entails implementing a series of protective mechanisms such that if one mechanism fails to thwart an attack, another will provide a backup defense. Software vulnerabilities can exist at each of the components of an agency’s IT infrastructure, and no single technical solution can successfully protect against all attacks that exploit these vulnerabilities. By utilizing the strategy of defense-in-depth, agencies can reduce the risk of a successful cyber attack. A layered

²⁴Buffer overflows occur when programs do not adequately check input for appropriate length. Thus, any unexpected input “overflows” onto another portion of the central processing unit’s executions stack. If this input is chosen judiciously by a rogue programmer, it can be used to launch code of the programmer’s choice.

approach to security can be taken by deploying both similar and diverse cybersecurity technologies at multiple layers of the IT infrastructure. Defense-in-depth also entails implementing an appropriate network configuration, which in turn can affect the selection and implementation of cybersecurity technologies—including automated patch management tools and services.²⁵

Configuration Management and Contingency Planning Can Be Used to Mitigate Risks

FISMA requires each agency to develop specific system configuration requirements that meet its own needs and ensure compliance with them, including maintaining up-to-date patches. In addition, industry best practices and federal guidance recognize the importance of configuration management when developing and maintaining a system or network to ensure that additions, deletions, or other changes to a system do not compromise the system's ability to perform as intended. Several agencies emphasized the need for a centralized entity within the agency that is responsible for the administration and control of the entire configuration management process, which includes patch management. In addition to ensuring a uniform and consistent implementation of all patches and updates on a timely basis, a centralized entity can help foster good communication between agency components and ensure implementation of necessary patches. Through effective configuration management, agencies can define and track the composition of a system to ensure that an unauthorized change is not introduced.

FISMA also requires that agencies' information security programs include plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency. Contingency plans provide specific instructions for restoring critical systems, including such elements as arrangements for alternative processing facilities, in case usual facilities are significantly damaged or cannot be accessed due to unexpected events such as temporary power failure, an accidental loss of files, or a major disaster. It is important that these plans be clearly documented, communicated to affected staff, and updated to reflect current operations.

²⁵A more comprehensive discussion of defense-in-depth and cybersecurity technologies can be found in U.S. General Accounting Office, *Information Security: Technologies to Secure Federal Systems*; [GAO-04-467](#) (Washington, D.C.: Mar. 9, 2004).

Ongoing Improvements in Patch Management Tools Can Further Assist Agencies

Security experts have noted the need for improving currently available patch management tools. Several patch management vendors have been working to do just that. For example, Microsoft has plans to improve its patching capabilities. Microsoft's newest version of Software Update Service is to be renamed Windows Update Services (WUS). WUS will be a server-based application for downloading and deploying patches. However, WUS has a limited scope and will support only specific applications.²⁶ The release of WUS has been delayed from this spring to later this year. Other patch management vendors have plans to expand their product capabilities and to support additional operating systems such as Linux, Unix, and Apache. Plans have also been discussed to save bandwidth by deploying patches from local repositories.

Research and Development of New Technologies Can Refine Software Code

Software security vulnerabilities can also be addressed through the research and development of automated tools to uncover hard-to-see security flaws in software code during the development phase. The code base of large commercial software products can literally be millions of lines. Microsoft Windows 2000 reportedly contains as many as 35 million lines. Moreover, because large products under development have changes to the code base every day, even during the final phase of development, code needs to be reviewed regularly. There are currently few automated tools that can be used during the code development phase to find the types of flaws that introduce overall security vulnerabilities to products.

Research and development in a wide range of other areas could also lead to more effective technologies to prevent, detect, and recover from attacks, as well as identify their perpetrators. These include more sophisticated firewalls to keep serious attackers out, better intrusion-detection systems that can distinguish serious attacks from nuisance probes and scans, systems that can isolate compromised areas and reconfigure while continuing to operate, and techniques to identify individuals responsible for specific incidents.

²⁶WUS will only support the following applications: Windows 2000 Service Pack 4 or higher; Windows Server 2003; Internet Information Services 5.5 and higher; and SQL Server 2000 SP 3 and higher, SQL Server 2003 or SQL Server Desktop Engine 2000.

Federal Buying Power Can Promote Higher Quality Software

The federal government can use its substantial purchasing power to demand higher quality software that would hold vendors more accountable for security defects in released products and provide incentives for vendors that supply low-defect products and products that are highly resistant to viruses.²⁷ The Corporate Information Security Working Group (CISWG), a group of representatives from IT trade and security organizations established last November by Representative Adam Putnam to develop a private-sector plan for improving cybersecurity in corporate America, recommends that federal agencies use their massive buying power to force IT vendors to build more secure products. In addition, CISWG recommends that insurers base the cost of cyber-risk insurance policies on a company's security posture to encourage adoption of best practices.

The federal government has already started to use its purchasing power to influence software vendors to deliver more secure systems. In September 2003, the Department of Energy—along with four other federal agencies and the Center for Internet Security—signed a contract with Oracle that requires the vendor to deliver the database to agencies with the security configurations installed. The contract could serve as a model to other federal agencies for leveraging their buying power with software vendors to require them to better secure their products.

DHS and Private-Sector Task Forces Are Taking Steps to Address Patch Management

The federal government—in collaboration with representatives from the private sector—have begun efforts in various components of patch management. In December 2003, NCSA and the National Cyber Security Partnership, a coalition of leading industry associations, established five task forces that include representatives from academia, trade associations, nonprofit organizations, companies, and federal government employees. Two of the task forces addressed patch management-related issues in their reports, including the need for better software engineering to reduce vulnerabilities, research and development of new technologies to improve software coding, and leveraging the federal government's buying power to promote higher quality software.

In April, the Security Across the Software Development Life Cycle Task Force issued a report with recommendations for improving software

²⁷The fiscal year 2004 information technology investment for the federal government is about \$59 billion.

security.²⁸ The task force recommended that software providers improve the development process by adopting practices for developing secure software. It also recommended that providers adhere to best practices that include thoroughly testing patches to confirm that errors are not introduced and to identify any dependencies on previously released patches, updates, or maintenance releases. Moreover, it recommended that providers make patches small, easy to install, and reversible, and that patches not introduce new product features or require reboots. The taskforce also developed a set of patch management guiding principles that include such criteria as establishing policies and procedures, defining a responsible person to monitor and enforce policy compliance, and adopting new technologies.

In April, The Technical Standards and Common Criteria Task Force also issued a recommendations report.²⁹ In the report, the task force's Research Working Group advised the federal government to fund research into the development of better code-scanning tools that can identify software defects. According to the task force, the tools to be developed should be able to operate on code developed in a variety of programming languages; handle millions of lines of code daily; support the development of large, complex applications; and run on many operating systems to support multiple development environments. Furthermore, the tools must also be suitable for products ranging from IT infrastructure to business applications, as well as for security products themselves. In addition, the working group recommended that the federal government require vulnerability analysis of products as a prerequisite to procuring software.

Conclusions

An ever-increasing number of software vulnerabilities resulting from flaws in commercial software products place federal operations and assets at considerable—and growing—risk. Patch management is an important element in mitigating these risks, as part of overall network configuration management and information security programs. Agencies have implemented common effective patch management practices inconsistently. Automated tools and services are available to facilitate agencies' implementation of selected patch management practices.

²⁸Improving Security Across the Software Development Lifecycle (April 1, 2004).

²⁹The National Cyber Security Partnership Technical Standards and Common Criteria Task Force, *Recommendations Report*, April 2004.

However, a number of common patch management obstacles remain. Additional steps can be taken by vendors, the security community, and the federal government to address the risk associated with software vulnerabilities and patch management challenges.

More refined agency reporting on key aspects of agencies' patch management practices could provide management and oversight organizations with better information for measuring the quality of agencies' patch management effectiveness. This reporting could facilitate agencies' progress in mitigating the risks caused by software vulnerabilities. Further, centralized services could provide a valuable resource for performing effective patch management practices as well as a venue for agencies to share information relevant to the various functionalities provided by different tools, IT infrastructures served, cost, effectiveness, and implementation issues and constraints.

Recommendations for Executive Action

We recommend that the Director of OMB take the following two actions. First, we recommend that the OMB Director provide guidance for agencies to report on key aspects of their patch management practices in their annual FISMA reports. This guidance could address measures relating to agencies' implementation of common patch management practices, such as documented policies and procedures, their testing of new patches in their specific computing environments prior to installation, and the frequency with which systems are monitored to ensure that patches are installed.

We also recommend that the OMB Director determine the feasibility of providing selected centralized patch management services to federal civilian agencies. OMB should coordinate with DHS to build on lessons learned regarding PADDC's limitations and weigh the costs against potential benefits. These services could potentially provide patch management functions such as centralized access to available tools and services, testing capabilities, and development of training.

Agency Comments

We received oral comments on a draft of our report from representatives of OMB's Office of Information and Regulatory Affairs and Office of General Counsel. These representatives generally agreed with our findings and recommendations. They plan to address key patch management practices in their FISMA reporting guidance to agencies, and believe sound configuration management is fundamental to successful patch

management. In addition, they acknowledge the potential benefits of centralized patch management services and will consider the feasibility of providing such services to federal agencies. Finally, they noted that, whether or not centralized patch management services are provided, ultimately it remains each agency and system owner's responsibility to maintain the security of their systems including ensuring timely patch updates.

As agreed with your offices, unless you publicly announce the contents of the report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies of this report to the Ranking Minority Members of the Committee on Government Reform and the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census and other interested parties. In addition, the report will be made available at no charge on GAO's Web site at <http://www.gao.gov>.

If you have any questions regarding this report, please contact me at (202) 512-3317 or Elizabeth Johnston, Assistant Director, at (202) 512-6345. We can also be reached by e-mail at dacey@gao.gov and johnstone@gao.gov, respectively. Key contributors to this report are listed in appendix II.



Robert F. Dacey
Director, Information Security Issues

Objectives, Scope, and Methodology

Our objectives were to determine the (1) reported status of 23 of the agencies under the CFO Act and DHS in performing effective patch management practices, (2) tools and services available to federal agencies to perform patch management, (3) challenges to performing patch management, and (4) additional steps that can be taken to mitigate the risks created by software vulnerabilities.

To determine the selected agencies' status in performing these practices, we first determined effective patch management practices by conducting an extensive search of professional IT security literature. We also reviewed research studies and reports about cybersecurity-related vulnerabilities to update information provided in our previous testimony and consulted our prior reports and testimonies on information security. In addition, we interviewed private-sector and federal officials about their patch management experiences and practices. We then developed a series of questions that were incorporated into a Web-based survey instrument. We pretested our survey instrument at one federal department, one component agency, and internally at GAO through our Chief Information Officer's office. We also corresponded with OMB to obtain and discuss the process for their data call of the Microsoft RPC and Cisco IOS vulnerabilities. For each agency to be surveyed, we identified the CIO office and notified each of our work and distributed a link to access the web-based survey instrument to each via e-mail. In addition, we discussed the purpose and content of the survey instrument with agency officials when requested. All 24 agencies responded to our survey. We did not verify the accuracy of the agencies' responses; however, we reviewed supporting documentation that agencies provided to validate their responses. We contacted agency officials when necessary for follow up. We then analyzed agency responses to determine the extent to which agencies were performing patch management practices.

Although this was not a sample survey and, therefore, there were no sampling errors, conducting any survey may introduce errors, commonly referred to as nonsampling errors. For example, difficulties in how a particular question is interpreted, in the sources of information that are available to respondents, or in how the data are entered into a database or were analyzed can introduce unwanted variability into the survey results. We took steps in the development of the survey instrument, the data collection, and the data analysis to minimize these nonsampling errors. For example, a survey specialist designed the survey instrument in collaboration with GAO staff with subject-matter expertise. Then, as stated earlier, it was pretested to ensure that the questions were relevant, clearly

stated, and easy to comprehend. When the data were analyzed, a second, independent analyst checked all computer programs. Because this was a Web-based survey, respondents entered their answers directly into the electronic questionnaire. This eliminated the need to have the data keyed into a database, thus removing an additional potential source of error.

To determine the tools and services available to federal agencies to perform patch management, we interviewed patch management software and service vendors as well as computer-security experts to discuss and examine their products' functions and capabilities. We also conducted literature searches and reviewed available documentation. We interviewed FedCIRC officials to discuss their experiences with PADC and other tools and services available to agencies. In addition, questions regarding patch management tools and services were included in the survey we sent to the 23 CFO agencies and to DHS.¹ Finally, we discussed with agencies the capabilities and limitations of the specific tools and services they utilized.

Finally, to determine the challenges to performing patch management and the additional steps that can be taken to mitigate the risks created by software vulnerabilities, we reviewed professional information technology security literature, examined available commercial software patch management tools and services, and solicited agencies' input on patch management challenges in our survey. We also interviewed relevant federal and private-sector officials and computer security experts. Finally, we reviewed reports prepared by the National Cyber Security Partnership subgroups tasked with identifying patch management challenges and developing recommendations.

We conducted our work in Washington, D.C., Charlotte, N.C., and Schaumburg, Ill., from September 2003 through May 2004, in accordance with generally accepted government auditing standards.

¹These 23 CFO departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Housing and Urban Development, Interior, Justice, Labor, State, Transportation, Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, Office of Personnel Management, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

Staff Acknowledgments

Acknowledgments

Key contributors to this report were Michael Fruitman, Elizabeth Johnston, Stuart Kaufman, Anjalique Lawrence, Min Lee, David Noone, and Tracy Pierson.

GAO's Mission

The General Accounting Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through the Internet. GAO's Web site (www.gao.gov) contains abstracts and full-text files of current reports and testimony and an expanding archive of older products. The Web site features a search engine to help you locate documents using key words and phrases. You can print these documents in their entirety, including charts and other graphics.

Each day, GAO issues a list of newly released reports, testimony, and correspondence. GAO posts this list, known as "Today's Reports," on its Web site daily. The list contains links to the full-text document files. To have GAO e-mail this list to you every afternoon, go to www.gao.gov and select "Subscribe to e-mail alerts" under the "Order GAO Products" heading.

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. General Accounting Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
 TDD: (202) 512-2537
 Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Public Affairs

Jeff Nelligan, Managing Director, NelliganJ@gao.gov (202) 512-4800
U.S. General Accounting Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Official Business
Penalty for Private Use \$300**

Address Service Requested

**Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00**

