United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

For Release on Delivery
Expected at 1:30 p.m. EDT
Wednesday, June 2, 2004

INFORMATION SECURITY

Agencies Face Challenges in Implementing Effective Software Patch Management Processes

Statement of Robert F. Dacey
Director, Information Security Issues

June 2, 2004

INFORMATION SECURITY

Agencies Face Challenges in Implementing Effective Software Patch Management Processes

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-816T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform

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--patch management--is critical to helping secure systems from attacks.

At the request of the Committee on Government Reform and this Subcommittee, GAO reviewed the (1) reported status of 24 selected agencies in performing effective patch management practices, (2) tools and services available to federal agencies, (3) challenges to this endeavor, and (4) additional steps that can be taken to mitigate risks created by software vulnerabilities. This testimony highlights the findings of GAO's report, which is being released at this hearing.

What GAO Recommends

In its report, GAO recommends that the Office of Management and Budget (OMB) instruct agencies to provide more refined information on their patch management practices in their annual reports and determine the feasibility of providing selected centralized services to federal civilian agencies. OMB concurs with these recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-04-816T.

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.

What GAO Found

Agencies are generally implementing certain common patch management-related practices, such as inventorying their systems and providing information security training. However, they are not consistently implementing other common practices. Specifically, not all agencies have established patch management policies and procedures. Moreover, not all agencies are testing all patches before deployment, performing documented risk assessments of major systems to determine whether to apply patches, or monitoring the status of patches once they are deployed to ensure that they are properly installed.

Commercial tools and services are available to assist agencies in performing patch management activities. These tools and services can make patch management processes more efficient by automating time-consuming tasks, such as scanning networks and keeping up-to-date on the continuous releases of new patches.

Nevertheless, agencies face significant challenges to implementing effective patch management. These include, among others,

- the high volume and increasing frequency of needed patches,
- patching heterogeneous systems,
- ensuring that mobile systems such as laptops receive the latest patches, and
- dedicating sufficient resources to assessing vulnerabilities and deploying patches.

Agency officials and computer security experts have identified several additional measures that vendors, the security community, and the federal government can take to address the risks associated with software vulnerabilities. These include, among others, adopting more rigorous software engineering practices to reduce the number of coding errors that create the need for patches, implementing successive layers of defense mechanisms at strategic points in agency information systems, and researching and developing new technologies to help uncover flaws during software development.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss patch management[1] and steps that agencies can take to mitigate information security risks resulting from software vulnerabilities. As you know, attackers may attempt to exploit such vulnerabilities, potentially causing significant damage to agencies' computer systems.

My testimony today will highlight the findings of a report requested by the Subcommittee and full Committee, which we are releasing today.[2] This report discusses: (1) the status of 23 of the agencies under the Chief Financial Officers (CFO) Act of 1990[3] and the Department of Homeland Security (DHS) in performing effective patch management, (2) tools and services available to assist federal agencies in this endeavor, (3) obstacles to performing effective patch management, and (4) additional steps that can be taken to mitigate the risks created by software vulnerabilities.

Our report is based on an extensive search of professional information technology (IT) security literature, research studies and reports about cybersecurity-related vulnerabilities (including our own), and the results of a Web-based survey of the 24 agencies that we conducted to determine their patch management practices. Our work was conducted from September 2003 through last month, in accordance with generally accepted government auditing standards.

Results in Brief

As our report discusses in detail, agencies are generally implementing certain important patch management-related

[1]Patch management is the process of applying software patches to correct flaws. A 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.

[2]U.S. General Accounting Office, *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO-04-706 (Washington, D.C.: June 2, 2004).

[3]31 USC Section 901.

practices, such as inventorying their systems and providing information security training. However, they are not consistently performing other critical practices, such as testing all patches before deployment to help determine whether the patch functions as intended and to ascertain its potential for adversely affecting an agency's system.

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

Agencies face several obstacles in implementing effective patch management practices, including (1) installing patches quickly while at the same time testing them adequately before installation, (2) patching heterogeneous systems, (3) ensuring that mobile systems receive the latest patches, (4) avoiding unacceptable downtime when patching systems that require a high degree of availability, and (5) dedicating sufficient resources to patch management.

Agency officials and computer security experts identified several additional steps that could be taken by vendors, the security community, and the federal government to assist agencies in overcoming such challenges. For example, more rigorous software engineering by vendors could reduce the number of vulnerabilities and the need for patches. In addition, the federal government could use its substantial purchasing power to influence software vendors to deliver more security systems.

Our report recommends that the Director, Office of Management and Budget (OMB), (1) instruct agencies to provide more refined information on their patch management practices in their annual Federal Information Security Management Act (FISMA) of 2002[4] 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

[4]Pub. L. 107-347, Title III, December 17, 2002.

initiated by the Federal Computer Incident Response Center (FedCIRC). OMB generally agrees 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

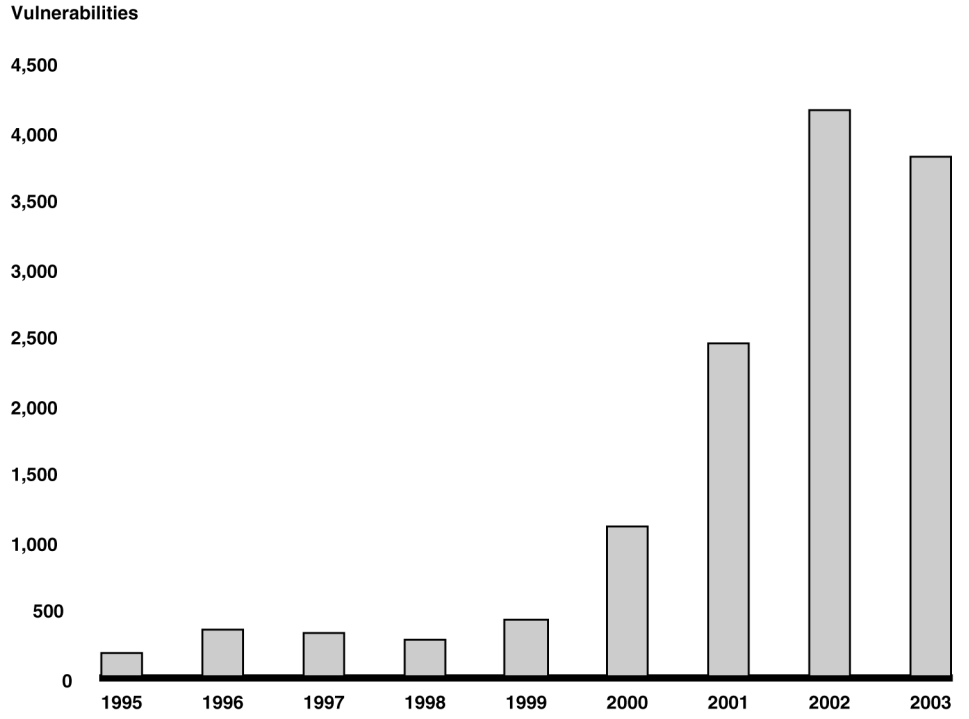
From 1995 through 2003, the CERT® Coordination Center (CERT/CC)[7] reported just under 13,000 security vulnerabilities that resulted from software flaws. Figure 1 illustrates the dramatic growth in security vulnerabilities during this period.

[5]Configuration 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.

[6]National Institute of 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).

[7]CERT/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 can cause major damage in attempting to exploit them. 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]

The sophistication and effectiveness of cyber attacks have steadily advanced. According to security researchers, reverse-engineering patches has become a leading method for exploiting vulnerabilities.

[8]A 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.

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. 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.

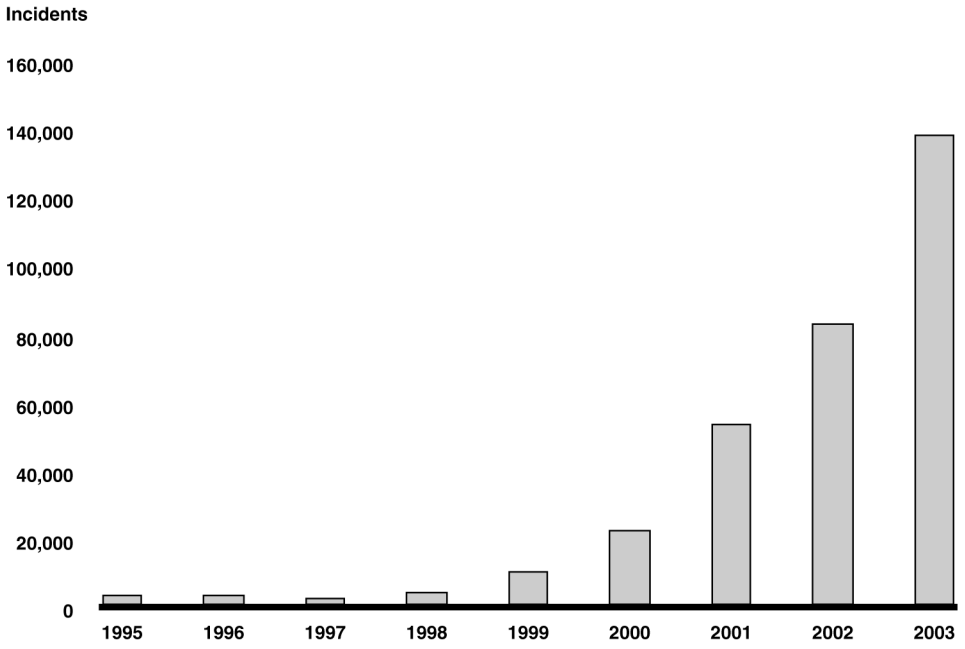
A spate of new worms has been released since February—most recently last month—and more than half a dozen new viruses were unleashed. The worms were variants of the Bagle and Netsky viruses. The Bagle viruses typically included an infected e-mail attachment containing the actual virus; the most recent versions have protected the infected attachment with a password, preventing anti-virus scanners from examining it. The recent Netsky variants attempted to deactivate two earlier worms and, when executed, reportedly make a loud beeping sound. Another worm known as Sasser, like the Blaster worm discussed later, exploits a vulnerability in the Microsoft Windows operating system, while the Witty worm exploits a flaw in certain Internet security software products.

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 over 137,500 in 2003. And these are only the reported attacks. The director of the CERT Centers has estimated that as much as 80 percent of actual security incidents go unreported, in most cases because

- there were no indications of penetration or attack,
- the organization was unable to recognize that its systems had been penetrated, or
- the organization was reluctant to report the attack.

Figure 2 shows the number of incidents reported to CERT/CC from 1995 through 2003.

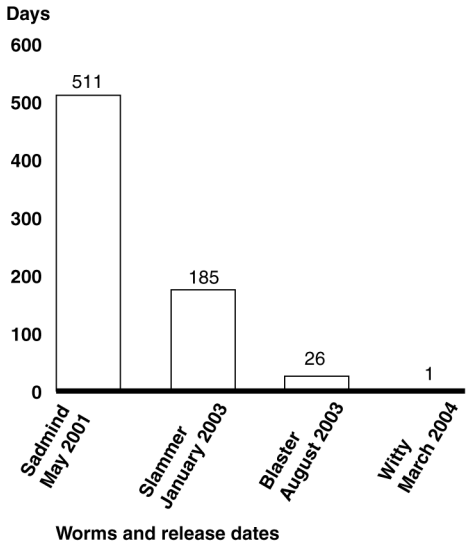
Figure 2: Computer Security Incidents, 1995–2003



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 recent Witty worm was released only a day after the announcement of the vulnerability it attacked. As figure 3 illustrates, in the last 3 years, the time interval between the announcement of a particular vulnerability and the release of its associated worm has diminished dramatically.

Figure 3: Time Interval between the Announcement of a Vulnerability and the Release of Its Associated Worm



Source: GAO.

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.[9] 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:

- On January 25, 2003, Slammer reportedly triggered a global Internet slowdown and caused considerable harm through

[9]Congressional Research Service, *The Economic Impact of Cyber Attacks* (Washington, D.C.: April 1, 2004).

network outages and other unforeseen consequences. As discussed in our April 2003 testimony on the security of federal systems and critical infrastructures, the worm reportedly shut down a 911 emergency call center, canceled airline flights, and caused automated teller machine failures.[10] 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 damage range between $1.05 billion and $1.25 billion.

- 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 its 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 reboot frequently. 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 the Blaster worm has infected at least 8 million Windows computers since last August.

[10]U.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.: April 8, 2003).

- On May 1 of this year, the Sasser worm 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 US-CERT (the United States Computer Emergency Readiness Team),[11] systems infected by this worm may suffer significant performance degradation. Sasser, like last year's Blaster, exploits a 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 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,

[11]A new service to function as the center for coordinating computer security preparedness and response to cyber attacks and incidents.

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

(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, it identifies the need for (1) a better–defined approach on disclosing vulnerabilities, to reduce their usefulness to hackers in launching an attack; (2) creating common test beds for applications widely used among federal agencies; and (3) establishing best practices for vulnerability remediation in areas such as training, use of automated tools, and patch management implementation processes.

US-CERT was created last September by DHS's National Cyber Security Division (NCSD) in conjunction with CERT/CC and the private sector. Specifically, US-CERT is intended to aggregate and disseminate cyber security 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.

Agencies Are Not Consistently Implementing Common Practices for Effective Patch Management

Common patch management practices—such as establishing and enforcing standardized 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.

Our survey results showed that the 24 agencies are implementing some practices for effective patch management, but not others. Specifically, all report that they have some level of senior executive involvement in the patch management process and cited the chief information security officer (CISO) as being the individual most involved in the patch management process. 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.

Other areas in which agencies report implementing common patch management practices are in performing a systems inventory and providing information security training. All 24 agencies reported that they develop and maintain an inventory of major information systems as required by FISMA and do so using a manual process, an automated tool, or an automated service. Additionally, 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.

However, agencies are inconsistent in developing patch management policies and procedures, testing of patches, monitoring systems, and performing risk assessments. Specifically, not all agencies have established patch management policies and procedures. Eight of the 24 surveyed agencies report having no policies and 10 do not have procedures in place. Additionally, most agencies are not testing all patches before deployment. Although all 24 surveyed agencies reported that they test some patches against their various systems configurations before deployment, only 10 agencies reported testing all patches, and 15 agencies reported that they do not have any testing policies in place. Moreover, although all 24 agencies indicated that they perform some monitoring activities to assess their network environments and determine whether patches have been effectively applied, only 4 agencies reported that they monitor all of their systems on a regular basis. Further, 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. Without consistent implementation of patch management practices, agencies are at

increased risk of attacks that exploit software vulnerabilities in their systems.

More refined 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 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 keeping current on the continuous flow of new patches.

Commercially available tools and services 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.

In addition to automated tools and services, agencies can use other methods to assist in their patch management activities. For example, although labor-intensive, 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. 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. 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.

We have previously 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.[13] According to FedCIRC officials, this service was terminated on February 21, 2004, for a variety of reasons, including low levels of usage. In the absence of this service, agencies are left to independently perform all components of effective patch management. A centralized resource that incorporates lessons learned from PADC's limitations could provide standardized services, such as testing of patches and a patch management training curriculum.

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

Significant Obstacles to Effective Patch Management Remain

Security experts and agency officials have identified several obstacles to implementing effective patch management; these include the following:

- High volume and increasing frequency of patches. 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. As increasingly virulent computer worms have demonstrated, agencies need to keep systems updated with the latest security patches.
- Patching heterogeneous systems. Variations in platforms, configurations, and deployed applications complicate agencies' patching processes. Further, their unique IT infrastructures can make it challenging for agencies to determine which systems are affected by a software vulnerability.
- Ensuring that mobile systems receive the latest patches. Mobile computers—such as laptops, digital tablets, and personal digital assistants—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.
- Avoiding unacceptable downtime when patching systems that require high availability. 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, particularly for critical systems that must be continuously available.
- Dedicating sufficient resources to patch management. 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.

Additional Steps Can Be Taken to Mitigate Risks

As with the challenges to patch management identified by agencies, our report also identified a number of steps that can be taken to address the risks associated with software vulnerabilities. These include:

- Better software engineering. More rigorous engineering practices, including 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.
- Implementing "defense-in-depth." 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 fails to thwart an attack, another will provide a backup defense.
- Using configuration management and contingency planning. 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. 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, accidental loss of files, or major disaster.
- Ongoing improvements in patch management tools. Security experts have noted the need for improving currently available patch management tools. Several patch management vendors have been working to do just that.

- Research and development of new technologies. 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.
- Federal buying power. 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.

In addition, DHS and private-sector task forces are taking steps to address patch management. For example, in April, two task forces established by DHS's NCSD and the National Cyber Security Partnership in December 2003 addressed patch management-related issues in their reports. The Security Across the Software Development Life Cycle Task Force recommended that software providers improve the development process by adopting practices for developing secure software.[14] The National Cyber Security Partnership Technical Standards and Common Criteria Task Force advised the federal government to fund research into the development of better code-scanning tools that can identify software defects.[15]

— — — — —

In summary, the 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 effective patch management practices inconsistently. While automated tools and

[14] *Improving Security Across the Software Development Life Cycle*, April 1, 2004.

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

services are available to facilitate agencies' implementation of selected patch management practices, several obstacles to effective patch management 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. Moreover, OMB's implementation of our recommendations to instruct agencies to provide more refined information on their patch management practices in their annual FISMA reports and determine the feasibility of providing selected centralized patch management services—with which they concurred— could improve agencies' abilities to oversee the effectiveness of their patch management processes.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time. Should you have any further questions about this testimony, please contact me at (202) 512-3317 or at daceyr@gao.gov.

Individuals making key contributions to this testimony included Michael P. Fruitman, Elizabeth Johnston, Stuart Kaufman, Anjalique Lawrence, Min Lee, David Noone, and Tracy Pierson.