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 10:00 a.m. EDT
Wednesday, September 10, 2003

INFORMATION SECURITY

Effective Patch Management is Critical to Mitigating Software Vulnerabilities

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-03-1138T

September 10, 2003

INFORMATION SECURITY

Effective Patch Management is Critical to Mitigating Software Vulnerabilities

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-1138T, testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, House Committee on Government Reform

Why GAO Did This Study

Attacks on computer systems—in government and the private sector—are increasing at an alarming rate, placing both federal and private-sector operations and assets at considerable risk. By exploiting software vulnerabilities, hackers can cause significant damage. While patches, or software fixes, for these vulnerabilities are often well publicized and available, they are frequently not quickly or correctly applied.

The federal government recently awarded a contract for a governmentwide patch notification service designed to provide agencies with information to support effective patching. Forty-one agencies now subscribe to this service.

At the request of the Chairman of the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, GAO reviewed (1) two recent software vulnerabilities and related responses; (2) effective patch management practices, related federal efforts, and other available tools; and (3) additional steps that can be taken to better protect sensitive information systems from software vulnerabilities.

www.gao.gov/cgi-bin/getrpt–GAO-03-1138T.

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.

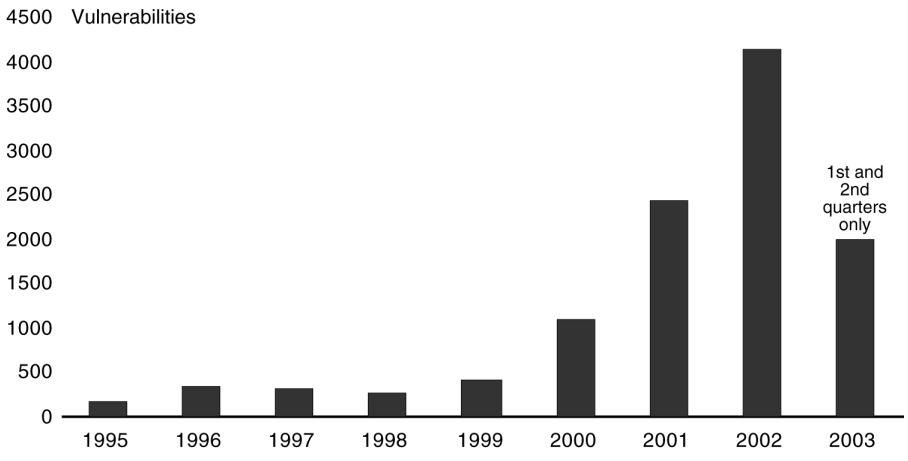
What GAO Found

The increase in reported information systems vulnerabilities has been staggering, especially in the past 3 years (see chart). Automated attacks are successfully exploiting such software vulnerabilities, as increasingly sophisticated hacking tools become more readily available and easier to use. The response to two recent critical vulnerabilities in Microsoft Corporation and Cisco Systems, Inc., products illustrates the collaborative efforts between federal entities and the information security community to combat potential attacks.

Patch management is one means of dealing with these increasing vulnerabilities to cybersecurity. Critical elements to the patch management process include management support, standardized policies, dedicated resources, risk assessment, and testing. In addition to working with software vendors and security research groups to develop patches or temporary solutions, the federal government has taken a number of other steps to address software vulnerabilities. For example, offered without charge to federal agencies, the federal patch notification service provides subscribers with information on trusted, authenticated patches available for their technologies. At present, the government is considering broadening the scope of these services and capabilities, along with the number of users. Other specific tools exist that can assist in performing patch management.

In addition to implementing effective patch management practices, several additional steps can be taken when addressing software vulnerabilities. Such steps include stronger software engineering practices and continuing research and development into new approaches toward computer security.

Security Vulnerabilities, 1995—First Half of 2003 (11,155 in the aggregate)



Source: Carnegie-Mellon University's CERT® Coordination Center.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to participate in the Subcommittee's hearing on recent cyber incidents and the role of software patch management[1] in mitigating the risks that these types of events will recur. Current incidents inundating the Internet, coupled with the increasing number and sophistication of attacks, place both federal and private-sector operations and assets at considerable risk. Several of these incidents exploited software vulnerabilities for which patches were already publicly available.

In my testimony today I will discuss (1) two recent software vulnerabilities and related responses; (2) effective patch management practices, related federal efforts, and other available tools; and (3) additional steps that can be taken to better protect sensitive information systems from software vulnerabilities.

In preparing for this testimony, we analyzed professional information technology security literature, including research studies and reports about cybersecurity-related vulnerabilities. We also interviewed private-sector and federal officials about their patch management experiences. And we analyzed relevant documents and interviewed officials of the Patch Authentication and Dissemination Capability (PADC) service and supporting contractors to determine the service's current capabilities and usage. Finally, we reviewed actions taken by PADC and agency officials in response to recent cybersecurity vulnerabilities. Our work was performed in accordance with generally accepted government auditing standards, from June to September 2003.

[1]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. Patch management is the process of effectively applying available patches.

Results in Brief

Since 1995, over 11,000 security vulnerabilities in software products have been reported. Along with these increasing vulnerabilities, the sophistication of attack technology has steadily advanced. Attacks such as viruses and worms[2] that once took weeks or months to propagate over the Internet now take only hours, or even minutes. In just the past 3 months, two critical and widespread vulnerabilities were identified in products from Microsoft Corporation and Cisco Systems, Inc. Federal agencies were affected by the Blaster and Welchia worms, which exploited the Microsoft vulnerability. The response to these recent events illustrates how federal entities are communicating and coordinating with software vendors and security research groups to combat such attacks.

Effective patch management, one means of dealing with these increasing security threats, includes several critical elements, such as top management support, standardized policies, dedicated resources, risk assessment, and testing. In the federal arena, the Department of Homeland Security now provides agencies with information on trusted, authenticated patches for their specific technologies without charge. This service, known as PADC, currently has 41 agency subscribers. Other tools and resources also exist that can assist in performing patch management functions.

Patch management is but one—albeit important and essential—component in the protection of systems from security vulnerabilities. However, in the longer term, the nation's ability to withstand attacks may ultimately come from more rigorous software engineering practices and better tools and technologies. My statement today will highlight steps we can take now and in the future to help reduce our vulnerability to cyber intrusion.

Background: Vulnerabilities and Exploits

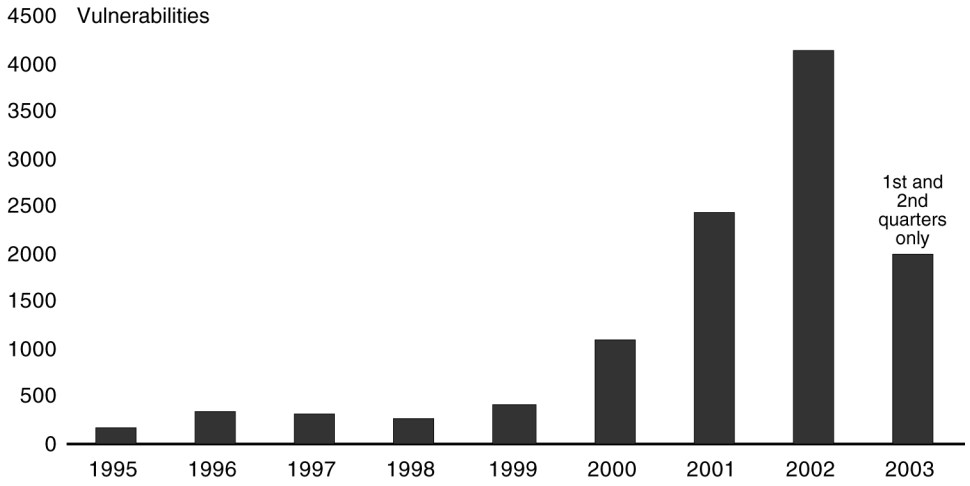
Flaws in software code that could cause a program to malfunction generally result from programming errors that occur during software development. The increasing complexity and size of software programs contribute to the growth in software flaws. For example, Microsoft Windows 2000 reportedly contains 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

[2]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.

create security vulnerabilities,[3] the potential for these errors reflects the difficulty and complexity involved in delivering trustworthy code.[4] By exploiting software vulnerabilities, hackers and others who spread malicious code can cause significant damage, ranging from Web site defacement 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.

Between 1995 and the first half of 2003, the CERT® Coordination Center[5] (CERT/CC) reported 11,155 security vulnerabilities that resulted from software flaws. Figure 1 illustrates the dramatic growth in security vulnerabilities over these years.

Figure 1: Security Vulnerabilities, 1995—first half of 2003



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

The growing number of known vulnerabilities increases the number of potential attacks created by the hacker community. As vulnerabilities are discovered, attackers may attempt to exploit them. Attacks can be launched against specific targets or widely distributed through viruses and worms.

[3] A vulnerability is the existence of a flaw or weakness in hardware or software that can be exploited resulting in a violation of an implicit or explicit security policy.

[4] National 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).

[5] The 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.

Worms and viruses are commonly used to launch denial-of-service attacks, which generally flood targeted networks and systems with so much transmission of data that regular traffic is either slowed or completely interrupted. Such attacks have been utilized ever since the groundbreaking Morris worm, which brought 10 percent of the systems connected to Internet systems to a halt in November 1988. In 2001, the Code Red worm used a denial-of-service attack to affect millions of computer users by shutting down Web sites, slowing Internet service, and disrupting business and government operations.[6] This type of attack continues to be used by recent worms, including Blaster, which I will discuss further later in my testimony.

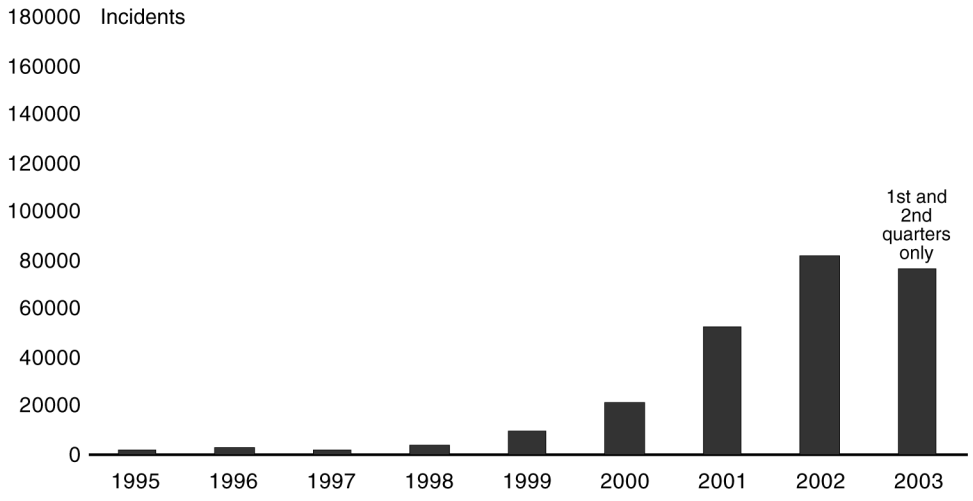
The sophistication and effectiveness of cyber attack have steadily advanced. Because automated tools now exist, CERT/CC has noted, attacks that once took weeks or months to propagate over the Internet now take just hours, or even minutes. Code Red achieved an infection rate of over 20,000 systems within 10 minutes, foreshadowing more damaging and devastating attacks. Indeed, earlier this year, the Slammer worm, which successfully attacked at least 75,000 systems, became the fastest computer worm in history, infecting more than 90 percent of vulnerable systems within 10 minutes.

Frequently, skilled hackers develop exploitation tools and post them on Internet hacking sites. These tools are then readily available for others to download, allowing even inexperienced programmers to create a computer virus or to literally point and click to launch an attack. According to a NIST publication, 30 to 40 new attack tools are posted to the Internet every month.[7]

The threat to systems connected to the Internet is illustrated by the increasing number of computer security incidents reported to CERT/CC. This number rose from just under 10,000 in 1999 to over 52,000 in 2001, to about 82,000 in 2002, and to over 76,000 for the first and second quarters of 2003. And these are only the incidents that are reported. According to the Director of CERT/CC, as much as 80 percent of actual incidents go unreported, in most cases because the organization was either unable to recognize that its systems had been penetrated (because there were no indications of penetration or attack) or because it was reluctant to report an incident. Figure 2 illustrates the number of incidents reported to CERT/CC from 1995 through the second quarter of 2003.

[6]U.S. General Accounting Office, *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures,* GAO-01-1073T (Washington D.C.: August 29, 2001).
[7]U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk,* GAO-01-751 (Washington D.C.: August 13, 2001).

Figure 2: Information Security Incidents, 1995—first half of 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 Blaster worm was released almost simultaneously with the announcement of the vulnerability it exploited.

Successful attacks on unpatched software vulnerabilities have caused billions of dollars in damage. Following are examples of significant damage caused by worms that could have been prevented had 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.

- On January 25, 2003, Slammer triggered a global Internet slowdown and caused considerable harm through network outages and other unforeseen consequences. As we discussed in our April testimony, the worm reportedly shut down a 911 emergency call center, canceled airline flights, and caused automated teller machine (ATM) failures.[8] 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

[8]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).

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 the 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, some of Microsoft's own systems were infected by Slammer.

In addition to understanding the threat posed by security vulnerabilities, it is useful to understand the process of vulnerability identification and response. In general, when security vulnerabilities are discovered, a process is initiated to effectively address the situation through appropriate reporting and response. 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 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 the Federal Computer Incident Response Center (FedCIRC) and CERT/CC, to discuss and plan remediation and response efforts.

After a vulnerability is validated, the software vendor develops and tests a patch and/or workaround. A workaround may entail blocking access to or disabling vulnerable programs.

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 where 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. When a worm or virus is reported that exploits a vulnerability, virus detection software vendors also participate in the process. Such vendors develop and make available to their subscribers downloadable "signature files" that are used, in conjunction with their software, to identify and stop the virus or worm from infecting systems protected by their software. The Organization for Internet Safety (OIS), which consists of leading security researchers and vendors, recently issued a voluntary framework for vulnerability reporting and response.[9]

[9]Organization for Internet Safety, *Guidelines for Security Vulnerability Reporting and Response, Version 1.0* (July 2003).

Collaborative Response to Two Recent Software Vulnerabilities

Recently, two critical vulnerabilities were discovered in widely used commercial software products. The federal government and the private-sector security community took steps, described below in chronological order, to collaboratively respond to the threat of potential attacks against these vulnerabilities.

Microsoft Remote Procedure Call Vulnerability Exploited by Hacker

Last Stage of Delirium Research Group discovered a security vulnerability in Microsoft's Windows Distributed Component Object Model (DCOM)[10] Remote Procedure Call (RPC)[11] interface. This vulnerability would allow an attacker to gain complete control over a remote computer.

- On June 28, 2003, the group notified Microsoft about the RPC vulnerability. Within hours of being notified, Microsoft verified the vulnerability.
- On July 16, Microsoft issued a security bulletin publicly announcing the critical vulnerability and providing workaround instructions and a patch.
- The following day, CERT/CC issued its first advisory.
- Nine days after Microsoft's announcement, on July 25, Xfocus, an organization that researches and demonstrates security vulnerabilities, released code that could be used to exploit the vulnerability.
- On July 31, CERT/CC issued a second advisory reporting that multiple exploits had been publicly released, and encouraged all users to apply the patches.
- On August 11, 2003, the Blaster worm (also known as Lovsan) was launched to exploit this vulnerability. When the worm is successfully executed, it can cause the operating system to crash. Experts consider Blaster, which affected a range of systems, to be one of the worst exploits of 2003. 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

[10]Distributed Component Object Model (DCOM) allows direct communication over the network between software components.
[11]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.

international arenas have also been affected. The worm was programmed to launch a denial-of-service attack on Microsoft's Windows Update Web site www.windowsupdate.com (where users can download security patches) on August 16. Microsoft preempted the worm's attack by disabling the Windows Update Web site.

- On August 14, two variants to the original Blaster worm were released. Federal agencies reported problems associated with these worms to FedCIRC.

- On August 18, Welchia, a worm that also exploits this vulnerability, was reported. Among other things, it attempts to apply the patch for the RPC vulnerability to vulnerable systems, but reportedly creates such high volumes of network traffic that it effectively denies services in infected networks. Media reports indicate that Welchia affected several federal agencies, including components of the Departments of Defense and Veterans Affairs.

  The federal government's response to this vulnerability included coordination with the private sector to mitigate the effects of the worm.

- On July 17, FedCIRC issued an advisory to encourage federal agencies to patch the vulnerability, followed by several advisories from the Department of Homeland Security (DHS).

- The following week, on July 24, DHS issued its first advisory to heighten public awareness of the potential impact of an exploit of this vulnerability.[12]

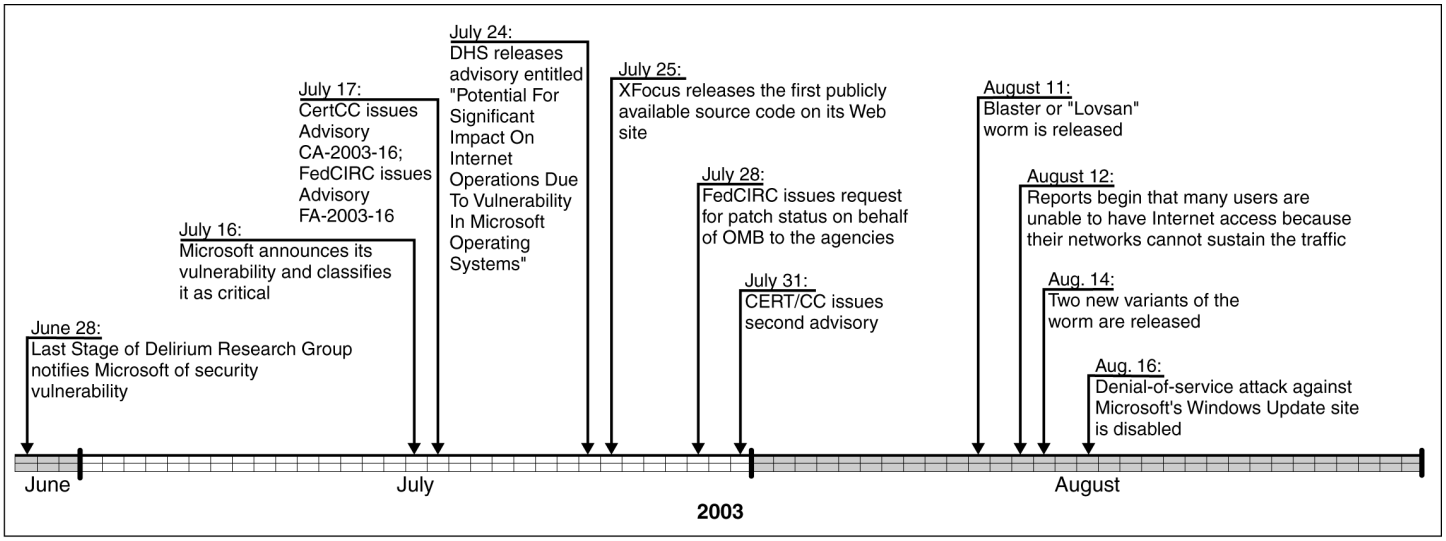
- On July 28, on behalf of the Office of Management and Budget (OMB), FedCIRC requested that federal agencies report on the status of their actions to patch the vulnerability.

- From August 12 to August 18, DHS's National Cyber Security Division hosted several teleconferences with federal agencies, CERT/CC, and Microsoft.

Figure 3 is a timeline of selected responses to the Blaster Internet worm.

[12]Department of Homeland Security, *Potential For Significant Impact On Internet Operations Due To Vulnerability In Microsoft Operating Systems* (Washington, D.C.: July 24, 2003).

Figure 3: Event Timeline for the Blaster Internet Worm



Source: GAO.

Based on an analysis of the agencies reported actions, as requested on July 28, FedCIRC indicated that many respondents had completed patch installation on all systems at the time of their report and that only a minimal number of infections by the Blaster worm were reported.

Cisco IOS Vulnerability Exploits Attempted

Cisco Systems, Inc., which controls approximately 82 percent of the worldwide share of the Internet router[13] market, discovered a critical vulnerability in its Internet operating system (IOS) software. This vulnerability 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.

- On July 16, 2003, Cisco issued a security bulletin to publicly announce the critical vulnerability in its IOS software, and provide workaround instructions and a patch. Cisco had planned to officially notify the public of the vulnerability on July 17, but early media disclosure led them to announce the vulnerability a day earlier. In addition, FedCIRC issued advisories to federal agencies and DHS advised private-sector entities of the vulnerability. In the week that the vulnerability was disclosed, FedCIRC, OMB, and DHS's National Cyber Security Division held a number of teleconferences with representatives from the executive branch.

[13]Routers are devices that forward Internet and network traffic between networks and are critical to their operation.

- On July 17, OMB requested that federal agencies report to CERT/CC on the status of their actions to patch the vulnerability by July 24.

- On July 18, DHS issued an advisory update in response to an exploit that was posted online, and OMB moved up the agencies' reporting deadline to July 22.

CERT/CC has received reports of attempts to exploit this vulnerability, but as of September 5, no incidents have yet been reported.

Patch Management: A Critical Process for Mitigating Cyber Vulnerabilities

Patch management is a process used to help alleviate many of the challenges involved with securing computing systems from attack. It is a component of configuration management[14] that includes acquiring, testing, and applying patches to a computer system. I will now discuss common patch management practices, federal efforts to address software vulnerabilities in agencies, and services and tools to assist in carrying out the patch management process.

Common Practices for Effective Patch Management

Effective patch management practices have been identified in security-related literature from several groups, including NIST, Microsoft,[15] patch management software vendors, and other computer-security experts. Common elements identified include the following:

- **Senior executive support**. Management recognition of information security risk and interest in taking steps to manage and understand risks, including ensuring that appropriate patches are deployed, is important to successfully implementing any information security–related process and ensuring that appropriate resources are applied.

- **Standardized patch management policies, procedures, and tools.** Without standardized policies and procedures in place, patch management can remain an ad-hoc process—potentially allowing each subgroup within an entity to implement patch management differently or not at all. Policies provide the foundation for ensuring that requirements are communicated across an entity. In addition, selecting and implementing appropriate patch management tools is an important consideration for facilitating effective and efficient patch management.

[14]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.

[15]Microsoft Corporation, *Solutions for Security, Solutions for Management: The Microsoft Guide to Security Patch Management* (Redmond, WA: 2003).

- **Dedicated resources and clearly assigned responsibilities.** It is important that the organization assign clear responsibility for ensuring that the patch management process is effective. NIST recommends creating a designated group whose duties would include supporting administrators in finding and fixing vulnerabilities in the organization's software. It is also important that the individuals involved in patch management have the skills and knowledge needed to perform their responsibilities, and that systems administrators be trained regarding how to identify new patches and vulnerabilities.

- **Current technology inventory**. Creating and maintaining a current inventory of all hardware equipment, software packages, services, and other technologies installed and used by the organization is an essential element of successful patch management. This systems inventory assists in determining the number of systems that are vulnerable and require remediation, as well as in locating the systems and identifying their owners.

- **Identification of relevant vulnerabilities and patches**. It is important to proactively monitor for vulnerabilities and patches for all software identified in the systems inventory. Various tools and services are available to assist in identifying vulnerabilities and their respective patches. Using multiple sources can help to provide a more comprehensive view of vulnerabilities.

- **Risk assessment**. When a vulnerability is discovered and a related patch and/or alternative workaround is released, the entity should consider the importance of the system to operations, the criticality of the vulnerability, and the risk of applying the patch. Since some patches can cause unexpected disruption to entities' systems, organizations may choose not to apply every patch, at least not immediately, even though it may be deemed critical by the software vendor that created it. The likelihood that the patch will disrupt the system is a key factor to consider, as is the criticality of the system or process that the patch affects.

- **Testing**. Another critical step is to test each individual patch against various systems configurations in a test environment before installing it enterprisewide to determine any impact on the network. Such testing will help determine whether the patch functions as intended and its potential for adversely affecting the entity's systems. In addition, while patches are being tested, organizations should also be aware of workarounds, which can provide temporary relief until a patch is applied. Testing has been identified as a challenge by government and private-sector officials, since the urgency in remediating a security vulnerability can limit or delay comprehensive testing. Time pressures can also result in software vendors' issuing poorly written patches that can degrade system performance and require yet another patch to remediate the problem. For instance, Microsoft has admittedly issued security patches that have been recalled because they have caused systems to crash or are too large for a computer's capacity. Further, a complex, heterogeneous systems

environment can lengthen this already time-consuming and time-sensitive process because it takes longer to test the patch in various systems configurations.

- **Distributing patches.** Organizations can deploy patches to systems manually or by using an automated tool. One challenge to deploying patches appropriately is that remote users may not be connected at the time of deployment, leaving the entity's networks vulnerable from the remote user's system because they have not yet been patched. 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.

- **Monitoring through network and host vulnerability scanning**. Networks can be scanned on a regular basis to assess the network environment, and whether patches have been effectively applied. Systems administrators can take proactive steps to preempt computer security incidents within their entities by regularly monitoring the status of patches once they are deployed. This will help to ensure patch compliance with the network's configuration.

Federal Efforts to Address Software Vulnerabilities

The federal government has taken several steps to address security vulnerabilities that affect federal agency systems, including efforts to improve patch management. NIST has taken a number of steps, including, as I previously mentioned, providing a handbook for patch management. In addition, NIST offers a source of vulnerability data, which I will discuss later in this testimony. Further, in accordance with OMB's reporting instructions for the first year implementation of the Federal Information Security Management Act (FISMA), maintaining up-to-date patches is a part of FISMA's system configuration requirements. As such, OMB requires that agencies report how they confirm that patches have been tested and installed in a timely manner.[16] In addition, certain governmentwide services are offered to federal agencies to assist them in ensuring that software vulnerabilities are patched. For example, FedCIRC was established to provide a central focal point for incident reporting, handling, prevention, and recognition for the federal government. Its purpose is to ensure that the government has critical services available in order to withstand or quickly recover from attacks against its information resources.

In addition, for the two recent vulnerabilities just discussed in my testimony, OMB and FedCIRC held teleconferences with agency Chief information officers to discuss vulnerabilities and request that agencies

[16] *Title III—Federal Information Security Management Act of 2002, 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.

report on the status of their actions to patch them. An OMB official indicated that they planned to hold meetings with agencies to discuss ways to improve communication of and followup on critical vulnerabilities, including addressing some of the challenges identified in the two recent exercises, such as delays in reaching key security personnel in certain instances.

FedCIRC also initiated PADC to provide users with a method of obtaining information on security patches relevant to their enterprise and access to patches that have been tested in a laboratory environment. The federal government offers PADC to federal civilian agencies at no cost. According to FedCIRC, as of last month, 41 agencies were using PADC. Table 2 lists its features and benefits, as reported by FedCIRC. OMB reported that while many agencies have established PADC accounts, actual usage of those accounts is extremely low.

Table 2: Reported Features and Benefits of the Patch Authentication and Dissemination Capability

Features	Benefits
• Authorized government users subscribe from a secure Web interface.	• Notifications to subscribers will occur when a patch is available for subscriber-selected systems or applications.
• Subscribers create customized notification profiles, including operating systems, firewalls, routers, antivirus software, intrusion-detection systems, and servers.	• FedCIRC will ensure that the patch originates from a reliable source.
• Subscribers are notified when new threats or vulnerabilities are discovered; notifications are updated as vendor patches are released and authenticated.	• FedCIRC will validate that the patch eliminates the intended vulnerability.
• Subscribers may visit a secure site to download validated patches.	• All aspects of the system are secure from subscriber information to the secure download of patches.
• Subscribers may contact the PADC Help Desk to verify information or to seek assistance.	• Single consolidated source for all patch updates. • No cost to federal civilian government agencies.

Source: FedCIRC.

To participate in PADC, subscribers (who could be one or more individuals within an agency) receive an account license that allows them to receive notifications and log into the secure Web site to download the patch. To establish an account, each subscriber must set up a profile defining the technologies that they use. The profiles act much like a filtering service and allow PADC to notify agencies of only the patches that pertain to their systems. The profiles do not include system–specific information because of the sensitivity of that information. Subscribers using PADC receive notification of threats, vulnerabilities, and the availability of patches on the basis of the submitted profiles. They are notified by E-mail or pager message that a vulnerability or patch has been posted to a secure Web site that affects one or all of their systems.

When a patch is identified, FedCIRC, through contractor support, ensures that it originates from a reliable source. The patch is then tested on a system to which it applies. The installation of the patch and the operation of the system are monitored to ensure that the patch causes no problem. Next, if an exploit had been developed, exploit testing is performed to ensure that the patch fixes the vulnerability. Any issues identified with a patch are summarized and provided to the users. The validated patch is then uploaded to PADC servers and made available to users. A patch is considered validated when it has been downloaded from a trusted source, authenticated, loaded onto an appropriate system, tested, exploit–tested, verified, and posted to the PADC server. This type of testing and validation is performed for over 60 technologies that, according to FedCIRC officials, account for approximately 80 percent of the technologies used by federal agencies. Also available is notification of patches that are not validated for over 25,000 additional technologies.

According to FedCIRC officials, high-priority patches are to be tested and posted on the PADC server within the same business day of availability. Medium- and low-priority patches are to be completed by the following business day, but are generally available sooner. However, because PADC has several early warning mechanisms in place and arrangements with software vendors, some patches may be available as soon as a vulnerability is made public. FedCIRC officials emphasize that although the contractor tests the security patches, these tests do not ensure that the patch can be successfully deployed in another environment; therefore, agencies still need to test the patch for compatibility with their own business processes and technology.

PADC offers a reporting capability that is hierarchical. Senior managers can look at their complete system and see which subsystems have been patched. These enterprisewide reports and statistics can be generated for a “reporting user” subscriber who has read-only capability within the system.

According to agency officials, there are limitations to the PADC service. Although it is free to agencies, only about 2,000 licenses or accounts are available because of monetary constraints. According to FedCIRC

officials, this requires them to work closely with participating agencies to balance the number of licenses that a single agency requires with the need to allow multiple agencies to participate. For example, the National Aeronautics and Space Administration initially requested over 3,000 licenses—one for each system administrator. Another agency, NIST, thought that each of its users should have his or her own PADC account. Another limitation is the level of services currently provided by PADC. At present, the government is considering broadening the scope of these services and capabilities, along with the number of users.

Services and Tools Also Provide Means for Improving Patch Management

Several services and automated tools are available to assist entities in performing the patch management function, including tools designed to be stand-alone patch management systems. In addition, systems management tools can be used to deploy patches across an entity's network. Some of the features in services and tools typically include 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 to easily manage patch deployment;
- scan a network to determine the status of the patches and other corrections made to network machines (hosts and/or clients);
- assess the machines against set criteria;
- access a database of patches;
- test patches;
- deploy effective patches; and
- report information to various levels of management about the status of the network.

Patch management vendors also offer central databases of the latest patches, incidents, and methods for mitigating risks before a patch can be deployed or a patch has been released. Some vendors provide support for multiple software platforms, such as Microsoft, Solaris, Linux, and others, while others focus on certain platforms exclusively, such as Microsoft.

Patch management tools can be either scanner–based (non agent) or agent–based. While scanner–based tools can scan a network, check for missing patches, and allow an administrator to patch multiple computers,

these tools are best suited for smaller organizations due to their inability to serve a large number of users without breaking down or requiring major changes in procedure. Another difficulty with scanner-based tools is that part-time users and turned-off systems will not be scanned.

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 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. The agents maintain information that can be reported when needed. Finally, some patch management tools are hybrids—allowing the user to utilize agents or not.

Instead of an automated stand-alone system, entities can also use other methods and tools to perform patch management. 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. While labor-intensive, this can be done. In addition, entities can employ systems management tools with patch-updating capabilities to deploy the patches. This method requires monitoring for the latest security alerts and patches. Entities may also need to develop better relationships with their vendors to be alerted to vulnerabilities and patches prior to public release. In addition, software vendors may provide automated tools with customized features to alert system administrators and users of the need to patch, and if desired, automatically apply patches.

A variety of resources are also available to provide information related to vulnerabilities and their exploits. As I mentioned earlier, one resource is CERT/CC, a major center for analyzing and reporting vulnerabilities as well as providing information on possible solutions. Another useful 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 vulnerability 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.

Many other organizations exist, including the Last Stage of Delirium Research Group, that research security vulnerabilities and maintain databases of such vulnerabilities. In addition, mailing lists, such as BugTraq, provide forums for announcing and discussing vulnerabilities, including information on how to fix them. In addition, Security Focus monitors thousands of products to maintain a vulnerability database and provide security alerts. Finally, vendors such as Microsoft and Cisco provide software updates on their products, including notices of known vulnerabilities and their corresponding patches.

Additional Steps That Can Be Taken

In addition to implementing effective patch management practices, several additional steps can be considered when addressing software vulnerabilities, including:

- deploying other technologies, such as antivirus software, firewalls, and other network security tools to provide additional defenses against attacks;
- employing more rigorous engineering practices in designing, implementing, and testing software products to reduce the number of potential vulnerabilities;
- improving tools to more effectively and efficiently manage patching;
- researching and developing technologies to prevent, detect, and recover from attacks as well as identify their perpetrators, such as 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; and
- ensuring effective, tested contingency planning processes and procedures.

Actions are already underway in many, if not all, of these areas. For example, CERT/CC has a research program, one goal of which is to try to find ways to improve technical approaches for identifying and preventing security flaws, for limiting the damage from attacks, and for ensuring that systems continue to provide essential services in spite of compromises and failures. Also, Microsoft recently initiated its Trustworthy Computing strategy to incorporate security-focused software engineering practices throughout the design and deployment of its software, and is reportedly considering the use of automated patching in future products.

— — — — —

In summary, it is clear from the increasing number of reported attacks on information systems that both federal and private-sector operations and assets are at considerable—and growing—risk. Patch management can be an important element in mitigating the risks associated with software vulnerabilities, part of overall network configuration management and information security programs. The challenge will be ensuring that a patch management process has adequate resources and appropriate policies, procedures, and tools to effectively identify vulnerabilities and patches that place an entity's systems at risk. Also critical is the capability to adequately test and deploy the patches, and then monitor progress to ensure that they work. Although this can currently be performed, the

eventual solution will likely come from research and development to better build security into software and tools from the beginning.

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 Shannin G. Addison, Michael P. Fruitman, Michael W. Gilmore, Sophia Harrison, Elizabeth L. Johnston, Min S. Lee, and Tracy C. Pierson.

(310507)