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.

September 10, 2003

INFORMATION SECURITY

Effective Patch Management is Critical to Mitigating Software Vulnerabilities

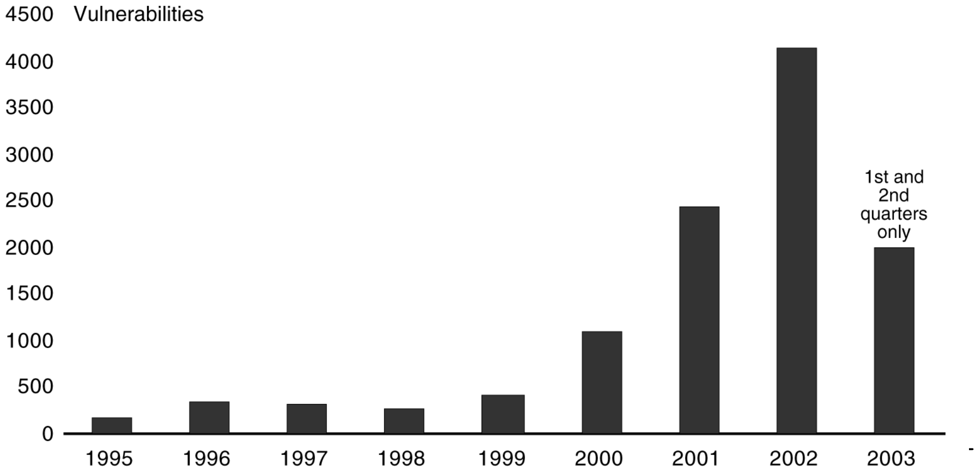
What GAO Found

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