June 2004

INFORMATION SECURITY

Continued Actions Needed to Improve Software Patch Management

GAO Accountability • Integrity • Reliability

Highlights

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.

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.