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.

June 2, 2004

INFORMATION SECURITY

Agencies Face Challenges in Implementing Effective Software Patch Management Processes

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.