Treasury Inspector General for Tax Administration

INTERNAL REVENUE SERVICE DATABASES CONTINUE TO BE SUSCEPTIBLE TO PENETRATION TESTS

Issued on December 14, 2007

Highlights

Highlights of Report Number: 2008-20-029 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) stores its taxpayer, financial, and other data in more than 2,100 databases. However, it continues to have recurring information security weaknesses that make its databases susceptible to penetration attacks. Due to the sensitivity of these data, the IRS could be a target for malicious users intent on committing identity theft and fraud. Theft of the data on these systems could also result in financial losses to the Federal Government

WHY TIGTA DID THE AUDIT

Since March 2003, TIGTA has identified and reported significant weaknesses in IRS database security controls. Previous reviews have demonstrated that control weaknesses could be exploited to gain access to sensitive taxpayer information and disrupt IRS computer operations.

This audit was initiated to determine whether databases used by IRS computer applications are secure from exploitation by unauthorized individuals.

WHAT TIGTA FOUND

High-risk weaknesses continue to exist, and sufficient efforts have not been taken to correct them. TIGTA scanned IRS networks and determined that 11 percent of the approximately 1,900 databases scanned had 1 or more installation accounts with a default or blank password. A total of 369 installation accounts had default or blank passwords; 26 contained powerful database administrator privileges.

While the IRS Computer Security Incident Response Center identifies password weaknesses on the systems it scans, it does not adequately scan all IRS databases. In addition, TIGTA found deficiencies in the process for reviewing Computer Security Incident Response Center scans that hamper the effectiveness and reporting accuracy of the review team's efforts.

Databases found with default or blank passwords during our scans include those that contain personally identifiable tax information. Malicious users can exploit accounts with default or blank passwords to steal taxpayer identities and carry out fraud schemes.

A majority of the IRS databases scanned do not have the latest software updates (patches) installed; 65 percent of the databases scanned needed to be updated, with more than 300 databases being outdated from 11 months to 20 months. As a result, outdated IRS databases were collectively susceptible to nearly 40,000 database vulnerabilities, one-half of which are considered high risk. These vulnerabilities include those used for common penetration attacks.

WHAT TIGTA RECOMMENDED

The Chief Information Officer should ensure security training is provided to employees with key security responsibilities; coordinate with other heads of office to emphasize the need for disciplinary actions for managers and employees who fail to fulfill their security responsibilities; improve the process for identifying and correcting accounts with blank or default passwords by expanding the scanning criteria, analyzing the Computer Security Incident Response Center scan results, and changing the methodology for determining repeat findings; and establish a process for monitoring database patch installations and updates to current versions of database software.

In their response to the report, IRS officials stated they agreed with the recommendations and plan to take appropriate corrective actions. The Chief Information Officer plans to update systems, processes, and training so employees are aware of the steps they must take to secure sensitive taxpayer data from unauthorized individuals.

READ THE FULL REPORT

To view the report, including the scope, methodology, and full IRS response, go to:

http://www.treas.gov/tigta/auditreports/2008reports/200820029fr.pdf.

Email Address: inquiries@tigta.treas.gov
Phone Number: 202-622-6500
Web Site: http://www.tigta.gov