



Treasury Inspector General for Tax Administration Office of Audit

AUTOMATED MONITORING IS NEEDED FOR THE VIRTUAL INFRASTRUCTURE TO ENSURE SECURE CONFIGURATIONS

Issued on September 18, 2013

Highlights

Highlights of Report Number: 2013-20-106 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Server virtualization is a technology that allows several “virtual” servers to run on one physical host. The conversion of physical servers to virtual servers improves hardware utilization, saves on electricity, and reduces server replacement costs. The IRS has made significant progress in expanding its virtual environment; however, more attention is needed to ensure that configurations are secure. Vulnerabilities in the virtual infrastructure could put taxpayer data at risk of unauthorized disclosure or loss.

WHY TIGTA DID THE AUDIT

This audit was initiated as part of our Fiscal Year 2013 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees. The overall objective of this review was to determine whether the IRS’s virtual environment is secure.

WHAT TIGTA FOUND

The IRS developed a comprehensive policy that establishes the minimum security controls to prevent unauthorized access to IRS information systems hosted in its virtual environment. A successful attack against a host can compromise all of the virtual servers residing on that host.

TIGTA tested 16 hosts and found that 12 (43 percent) of 28 required security controls were failed by three or more hosts. In addition, 10 (63 percent) of the 16 hosts were missing a total of 48 security patches. The IRS did not use an automated means to check that the security configuration settings were maintained in accordance with the IRS’s baseline configuration settings. Also, audit logs for the hosts were not collected and reviewed as required by IRS policy. Until an automated monitoring tool is implemented, the IRS will not be able to effectively monitor and maintain security configurations that are needed to secure the IRS virtual infrastructure and the sensitive data that reside on it.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure that the IRS: 1) implements an automated tool to ensure that host and vCenter™ settings remain in compliance with configuration standards; 2) applies patches to hosts timely in accordance with IRS policy; and 3) implements audit log collection and review on hosts and vCenters in accordance with IRS policy.

The IRS agreed with all of TIGTA’s recommendations and plans to: 1) procure and/or develop an automated tool, or adapt existing monitoring infrastructure, to report virtual host and vCenter compliance; 2) apply patches to hosts timely in accordance with IRS policy; and 3) develop audit plans and implement log file collection and review for both the hosts and vCenters.

READ THE FULL REPORT

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

<http://www.treas.gov/tigta/auditreports/2013reports/201320106fr.pdf>