U.S. International Trade Commission

Audit of Patch Management

OIG-AR-11-17

September 30, 2011

Office of Inspector General

The U.S. International Trade Commission is an independent, nonpartisan, quasi-judicial federal agency that provides trade expertise to both the legislative and executive branches of government, determines the impact of imports on U.S. industries, and directs actions against certain unfair trade practices, such as patent, trademark, and copyright infringement. USITC analysts and economists investigate and publish reports on U.S. industries and the global trends that affect them. The agency also maintains and publishes the Harmonized Tariff Schedule of the United States.

Commissioners

Deanna Tanner Okun, Chairman
Irving A. Williamson, Vice Chairman
Charlotte R. Lane
Daniel R. Pearson
Shara L. Aranoff
Dean A. Pinkert

UNITED STATES INTERNATIONAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20436

VIA ELECTRONIC TRANSMISSION

September 30, 2011 OIG-JJ-020

Chairman Okun:

This memorandum transmits the Office of Inspector General's final report Audit of Patch Management, OIG-AR-11-17. In finalizing the report, we analyzed management's comments on our draft report and have included those comments in their entirety in Appendix A.

This report contains four recommendations for corrective action. In the next 30 days, please provide me with your management decisions describing the specific actions that you will take to implement each recommendation.

Thank you for the courtesies extended to my staff during this audit.

Sincerely,

Philip M. Heneghan
Inspector General

Table of Contents

Results of Audit **1**

Areas for Improvement **1**

Area for Improvement 1: Use a single scanning tool to scan the Commission's entire network. 1

Area for Improvement 2: Implement a regular patching schedule for all servers. 2

Management Comments and Our Analysis **3**

Scope and Methodology **4**

Appendix A: Management Comments on Draft Report ..... **A**

Results of Audit

Has the USITC implemented an effective, comprehensive system to maintain patch levels?

Yes. The USITC has implemented an effective, comprehensive system to maintain patch levels.

The Commission uses a vulnerability scanner to scan the majority of its network infrastructure on a weekly basis. The Commission's 455 workstations, which are the most vulnerable and represent most of the systems on ITCNet, were missing a total of 868 patches, for an average of 1.9 High Severity patches per workstation. This is an improvement when compared to an audit last year that identified USITC workstations were missing an average of 80 High Severity patches. Many of the missing workstation patches were due to outdated systems used to connect to the National Business Center. This software requires that the Commission accept the risk of using outdated software to perform financial management functions. The seven workstations used for financial reporting exhibited an average of 16 missing High Severity patches per workstation, significantly skewing the total patching score. These seven workstations compose only 1.5% of the Commission's workstations, but resulted in 13% of the risk. The Commission has made commendable progress in implementing an effective patch management program.

We identified some areas that would support the Commission's efforts to improve its patching capabilities by consolidating its scanning efforts into a single tool that scans the entire network, and by implementing a patching schedule for all systems on its network.

Areas for Improvement

Area for Improvement 1:

Use a single scanning tool to scan the Commission's entire network.

The Commission should use a single tool to scan its entire network for vulnerabilities. It currently uses a tool to scan its workstations and specific network address ranges that host some of the servers on ITCNet; however, it is not using the same tool to scan all servers or ITCNet's entire network space.

The scanning tool has not been configured to perform complete scans of the Commission's networks. The Commission's internal network space has over 65,000 IP addresses, and only subsets of these IP addresses are scanned. In addition, the tool has not been configured to scan 40 non-Windows servers.

If the Commission does not scan the entirety of its network space, some systems could have unexpected but valid IP addresses on ITCNet and not be scanned.

Recommendation 1:

Shrink the available network IP space to make it possible for all IP space to be scanned on a weekly basis.

Recommendation 2:

Use one tool to scan all infrastructure.

Area for Improvement 2:

Implement a regular patching schedule for all servers.

To reduce its level of risk, the Commission has implemented regular patching for most systems, including Windows workstations and servers, and Linux servers.

We reviewed the patch status of 36 Linux servers. Thirty-four of these were missing an average of 5.9 packages, and the remaining two were missing 58 and 276 packages. During the audit, we found that different operational groups were implementing different server patching standards, resulting in the disparity between the majority of the servers and these two unpatched servers.

While most systems are being patched regularly, these two servers remained in production in an unpatched status for months, significantly increasing the risk to the network.

Recommendation 3:

Use a single vulnerability scanning tool to fully scan all IP network ranges in ITCNet.

Recommendation 4:

Patch all systems on a regular basis.

Management Comments and Our Analysis

On September 27, 2011, Chairman Deanna Tanner Okun provided management comments on the draft audit report. The Chairman agreed with our assessment that there are two areas for improvement, and recognized that the Commission can further improve its effective patch management system by implementing the recommendations detailed in the two areas for improvement. The Chairman's response is provided in its entirety as Appendix A.

Scope and Methodology

Scope:

The scope of this audit included all systems on all networks managed by the U.S. International Trade Commission.

Methodology:

1. Collect data identifying all network assets.
2. Collect existing vulnerability scans from all available network scanners.
3. Perform analysis of vulnerability scans, identifying patching patterns and potential outliers.
4. Perform delta analysis of network assets versus scanning ranges.
5. Identify systems not being scanned or patched consistently.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix A: Management Comments on Draft Report

Chairman

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

CO76-JJ-047

September 27, 2011

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Deanna Tanner Okun, Chairman

SUBJECT: Management Comments to the Inspector General's Draft Audit Report, "Audit of Patch Management"

I appreciate the opportunity to review the Inspector General's draft report, *Audit of Patch Management*, dated August 26, 2011, and to provide comments.

The Inspector General's draft report found that the Commission has implemented an effective, comprehensive system for patching its major IT platforms. The report, however, did reveal two areas for improvement: (1) the Commission could consolidate its scanning efforts into a single tool that scans the entire network, and (2) the Commission could implement a patching schedule for all systems on its network.

We agree with the findings. The Commission is dedicated to continuing our efforts on improving and maturing our patch management program. Thank you for reviewing the Commission's patch management program and making the recommendations to strengthen and broaden its effectiveness.

"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to perform complex mathematical calculations involving roots and powers quickly. The instrument was used by architects, engineers, and actuaries as a measuring device.

To Promote and Preserve the Efficiency, Effectiveness, and Integrity of the U.S. International Trade Commission

U.S. International Trade Commission
Office of Inspector General
500 E Street, SW
Washington, DC 20436

Office: 202-205-6542
Fax: 202-205-1859
Hotline: 877-358-8530
OIGHotline@USITC.gov