U.S. International Trade Commission

Audit of Security of Public-Facing Endpoints

OIG-AR-13-10

June 24, 2013

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

Irving A. Williamson, Chairman
Daniel R. Pearson
Shara L. Aranoff
Dean A. Pinkert
David S. Johanson
Meredith M. Broadbent

UNITED STATES INTERNATIONAL TRADE COMMISSION

OFFICE OF INSPECTOR GENERAL

WASHINGTON, DC 20436

June 24, 2013 IG-LL-009

Chairman Williamson:

This memorandum transmits the Office of Inspector General's final report, *Audit of Public-Facing Endpoints*, OIG-AR-13-10. This audit focused on whether the Commission blocks access to network ports that should not respond to the Internet. In finalizing this report, we analyzed management's comments to our draft report and have included those comments in their entirety as Appendix A.

This audit identified two problem areas that culminated in a lack of security for public-facing endpoints. This report presents three recommendations to address the identified problem areas. 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 the auditors during this review.

Philip M. Heneghan

Table of Contents

Results of Audit **1**

Problem Areas **2**

Problem Area 1: The Commission did not block access to ports that should not respond to the Internet. 2

Problem Area 2: The Commission did not perform ongoing scanning to detect responding ports. 3

Objective, Scope and Methodology **4**

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

Results of Audit

The purpose of this audit was to answer the question:

> Apart from its intrusion prevention systems, has the Commission secured its public-facing endpoints?

No. The Commission did not secure its public-facing endpoints.

To secure its public-facing endpoints, the Commission must block access to network ports that should not respond to the Internet.

The ITC's computer network has over 500 systems, consisting of servers, desktops, laptops, printers, phones, and network infrastructure devices. Every computer is connected to the network with a unique IP (Internet Protocol) address. For example, a desktop PC on the ITC network might have an address like 192.168.50.40. A typical Windows PC could have more than 20 responding ports. Each port serves a function; for instance, an Internet browser connects to port 80 to request web pages from a webserver, and email servers use port 25 to transfer messages. It would be normal for an unprotected network of 500 systems to present 10,000 responding ports, all potential targets for attack.

The goal of perimeter defense is to minimize the number and exploitability of responding ports, known as the "attack surface." A network with no responding ports is not a network: responding ports are required to communicate. Devices such as firewalls are configured to limit the number of ports exposed to the Internet, and newer technologies such as Intrusion Detection and Prevention Systems (IDPS) can provide additional protection.

When accessed from the Internet, ITC's network should have had 14 responding IP addresses and 26 responding ports to provide the services necessary to support USITC's business functions.

Our scan of responding network ports identified the following:

- 41 responding ports from 18 different IP addresses,
- 15 of 41 ports that should not have responded to our scans,
- 4 of 18 IP addresses were detected that should not have been visible, and
- Two ports responded with a telnet login prompt to a network device.

When we identified ports that should not have been responding, we immediately notified the CIO's office, who then took action to block Internet access to those ports.

We conducted two audits simultaneously. One audit examined the effectiveness of the Commission's perimeter defense and found that taken as a whole; the Commission's perimeter defense was effective. (*Report No…*) This audit examined a single component (responding ports) of the Commission's perimeter defense. As each component is strengthened, the Commission's defense as a whole is improved. Resolving the two problems we identified will reduce the risk to the Commission's network. These problem areas are: the Commission did not block access to ports that should not respond to the Internet, and it did not perform ongoing scanning to detect vulnerabilities. These problem areas are detailed below.

Problem Areas

Problem Area 1:
The Commission did not block access to ports that should not respond to the Internet.

When a device is installed on a high-risk, Internet-accessible network, it must be configured to provide the required functionality while limiting risk. This is typically managed by blocking Internet access to ports not necessary for required functionality.

We identified 15 open ports on the USITC network that should not have been accessible to the Internet. Two of these ports provided a login screen for direct access to network devices, as seen in the screenshot below:

```
*****************************************************************************
*     L E G A L   N O T I C E --  Y O U   M U S T   R E A D                 *
*****************************************************************************
*                                                                           *
*     You must have explicit permission to access or configure this         *
*      device.  All activities performed on this device are logged and      *
*     violations of this policy may result in criminal prosecution.         *
*                                                                           *
*****************************************************************************
*                                                                           *
* This system is for the use of authorized users only. Individuals using   *
*this computer system without authority, or in excess of their authority,  *
* are subject to having all of their activities on this system monitored   *
* and recorded by system personnel.                                         *
*                                                                           *
*                                                                           *
*  Anyone using this system expressly consents to such monitoring and is   *
* advised that if such monitoring reveals possible evidence of criminal    *
* activity, system personnel may provide the evidence of such monitoring   *
* to law enforcement officials.                                             *
*                                                                           *
*****************************************************************************
*         UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED          *
*****************************************************************************


User Access Verification

Username:
------------- [...]
```

This type of access should never be allowed to the Internet, especially for a network device. In this case, new hardware was installed on the Commission's network, but it was not configured to deny this type of access. A failure to secure network equipment increases the risk to the entire network supported by these devices.

Recommendation 1: Block ports that should not be exposed to the Internet.

Problem Area 2:
The Commission did not perform ongoing scanning to detect responding ports.

Networks and their systems evolve over time, either deliberately or by chance. Installation and maintenance of devices can result in the inadvertent exposure of ports that should not be accessible to the Internet. The best means to detect and enable the resolution of these problems is through thorough scanning of the devices before they are exposed to the Internet, and through routine scanning of the network perimeter to detect any ports that should not be open.

At the time of the audit, the Commission was not performing routine scanning of its perimeter. Because scanning was not being performed, CIO staff were unaware that ports were open that should not have been accessible from the Internet.

The best means of mediating this risk is through vulnerability scanning, on both a periodic basis and on-demand any time a change is made to the environment.

Recommendation 2: Perform scheduled, routine scanning of all perimeter devices on at least a monthly basis.

Recommendation 3: Perform perimeter device scans after new hardware or software is introduced to the ITC perimeter network.

Objective, Scope and Methodology

Objective:

- Apart from its intrusion prevention systems, has the Commission secured its public-facing endpoints?

Scope:

This audit documented all non-SMTP responding ports and corresponding IP addresses accessible from the Internet on ITCNet during the month of July, 2012. This audit enumerated the available points of access, and described the specific access methods for these access points.

Methodology:

1. The CIO whitelisted the scanning source address so scans would not be blocked by the Intrusion Prevention System.
2. Using the information provided by the Commission, we performed device service discovery using a toolset that included Nessus, Nmap, and applications within the BackTrack tool suite.
3. We analyzed and described accessible devices and services.
4. We compared accessible devices and services with those required to provide business services to the public.

Appendix A: Management Comments on Draft Report

Chairman

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

CO81-LL-009

May 31, 2013

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

FROM: Irving A. Williamson, Chairman

SUBJECT: Management Response to the Inspector General's "Audit of Security of Public-Facing Endpoints"

Thank you for your recent transmittal of the "Audit of Security of Public-Facing Endpoints" draft report, dated May 6, 2013, and for the opportunity to review it.

The audit's central determination was that the Commission has not secured its public-facing online endpoints. According to the report, this was because certain devices had not been fully configured to block access from the Internet and scanning practices were not being used to detect responding ports.

We agree with the findings and are in the process of instituting management decisions that will address the recommendations put forth in this report. Thank you, once again, for your thoughtful review and we look forward to working together to address this situation in a timely manner.

"Thacher's Calculating Instrument" developed by Edwin Thacher in the late 1870s. It is a cylindrical, rotating slide rule able to quickly 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: 202-205-6542
OIGHotline@USITC.gov