U.S. International Trade Commission

Audit of Patching

OIG-AR-14-02

November 12, 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.

UNITED STATES INTERNATIONAL TRADE COMMISSION

WASHINGTON, DC 20436

November 12, 2013 IG-LL-018

Chairman Williamson:

This memorandum transmits the Office of Inspector General’s final report, *Audit of the Commission’s Patching Process*, OIG-AR-14-02. This audit focused on whether the Commission’s process for patching systems was effective.

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 determined that the patching process was not effective and identified three problem areas.

This report presents seven recommendations to address the 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 Heneghan

Philip M. Heneghan
Inspector General

Table of Contents

Tables and Charts

Results of Audit

The purpose of this audit was to answer the question:

> Is the Commission's process for patching ITCNet systems effective?

No. The Commission's process for patching ITCNet systems was not effective.

In order to effectively patch its systems, the Commission's process should measure all of its systems for missing patches, rapidly apply missing patches, and inform executive management with a complete and accurate status.

Systems can include physical or virtual servers, laptops, desktops, tablets, printers, network switches, and other types of devices. When they are connected to the Commission's network, each of these systems has at least one IP address, and each detected IP address is referred to as a "host."

The process was not effective because 49% of detected hosts were not evaluated for missing patches, patches for High severity vulnerabilities were not applied in a timely manner, and the risk from missing patches was not effectively reported.

When software vendors identify problems with their applications or operating systems, they create and release updates to the software to resolves these issues. These updates are known as 'patches.' These patches are made available to the public, who install these patches to rectify the problems they are intended to solve. According to the CIO, 145,005 patches were applied to Commission workstations between January and August this year.

The majority of patches being released are designed to correct newly-identified security flaws. Systems without these patches are vulnerable to exploits from these security flaws, which could result in an intrusion by malicious individuals. Vulnerabilities defined as High severity identify those with the highest risk to the systems in question. Once a patch is released, the risk increases for systems that remain unpatched, because it has been publically announced that a flaw is present, and the software patch can be analyzed to precisely identify the nature of the security flaw. Malicious parties use this information to create new exploits if they aren't already available.

Patching systems is a primary means of securing systems and there are no effective substitutes for this basic security measure. In order to manage and reduce the risk to the organization, those responsible for managing its systems must continually track the patched status of those systems, and deploy patches as soon as they are made available. If systems are allowed to remain unpatched, the ease with which they can be attacked can nullify all other security measures in place at the organization.

In our analysis of the data provided by the OCIO, we found that 49% of detected hosts had not been scanned for missing patches. The table below describes two distinct sets of data for two different scanning weeks, one during the week of July 14th, and the other the week of August 4th. The number of hosts detected is subdivided into those fully measured for missing patches, and those that were not. For those that were measured, we provide an average number of High severity vulnerabilities per host.

Table 1: Scanning Results of Hosts

Description	Week of July 14	Week of August 4	Average
Hosts Detected	**867**	**847**	**857**
Hosts not measured	***407***	***431***	***419***
- *Hosts with no scan attempted*	*5*	*6*	*5.5*
- *Hosts with scan errors*	*402*	*425*	*413.5*
Hosts Measured	**460**	**416**	**438**
- Hosts Missing High severity patches	451	406	428.5
- Hosts Missing no High severity patch	9	10	9.5
Vulnerabilities Due to Missing Patches	**6152**	**2708**	**4430**
Average High Severity Vulnerabilities Per Host	**13.4**	**6.5**	**9.95**

For the hosts that were measured and found to be missing High severity patches, virtually all patches missing were more than a week old, and 21% of them were more than 1 year old. The average age of vulnerabilities due to missing patches is seen in the table below:

Table 2: Average Age of Vulnerabilities

Age of Missing Patches	Percentage of Vulnerabilities
Less than 7 days	0.3%
7-13 days	32.3%
14-90 days	28.3%
90-365 days	18.1%
More than 365 days	20.9%

The risk facing the Commission due to missing patches was not effectively reported. The Commission uses a formula that results in a target index score of 5, which implies that any number less than 5 indicates a secure network. Because the target score, or upper limit, is the log of a number, the target number is actually 100,000.

In our review of the two sets of the CIO's scan data, we found that on average, 438 hosts were scanned for missing patches. This means that an average, per-host passing score would be any number less than 228 (100,000/438). Since a score of 7 or more is a High vulnerability, the implication is that the Commission finds it acceptable to have 33 (228/7=33) High severity vulnerabilities per host.

The current method of reporting provides the Commission with a false sense of security and the stated goal would allow the risk to rise even more without the Commission becoming aware of an increased risk.

The three problem areas: (1) half of detected hosts were not evaluated for missing patches, (2) patches for High severity vulnerabilities were not applied in a timely fashion, and (3) risk due to missing patches was not effectively reported, are detailed below.

Problem Areas

Problem Area 1:

The Commission Did Not Measure Half of its Hosts for Missing Patches

An effective vulnerability management program requires knowing the patch status of all hosts. This is usually done by scanning the network and checking the patch status of each host on the network. It is not possible to effectively manage the patching process without a comprehensive measurement of status.

We reviewed two sets of data from scans performed the week of July 14th, and August 8th. We found that an average of 857 hosts were detected by the two sets of scans, but an average of 419 (49%) were not successfully measured for missing patches.

An overall contributing factor is that the Commission has self-imposed complexity by creating a single network with over 65,000 addresses, which is not a best practice. The decision to configure and maintain the network in this way has a number of negative consequences, one of which is that the network space is simply too large to be scanned on a frequent basis for missing patches. This resulted in a situation where not all hosts were being measured for missing patches on a continuous basis.

In order to detect missing patches, the scans must be configured to use login credentials to connect to each host and gather an inventory of installed software. If the credentials aren't provided, or if for some reason they fail, then the host will not be scanned for missing patches. The scanning software provided several indicators of this failure to scan for missing patches, including:

1. (51%) The local checks failed because the account used did not have sufficient privileges to read all the required registry entries.
2. (30%) It was not possible to connect to PIPE\winreg on the remote host. If the scanning software is going to be used to perform registry-based checks, the registry checks will not work because the 'Remote Registry Access' service (winreg) has been disabled on the remote host or cannot be connected to with the supplied credentials.
3. (19%) Other. Either some other error occurred, or the use of credentials was not attempted.

When scans cannot measure for missing patches, the hosts may appear clean; as if they have no vulnerabilities (are not missing patches). This leads to a false sense of security. The effect is that until these issues are identified and resolved, the Commission cannot know the risk to its network.

Recommendation 1: That the CIO shrink the network to facilitate at least weekly patch scanning of all hosts.

Recommendation 2: That the CIO implement alerts to identify all hosts that fail the patch measurement process.

Recommendation 3: That the CIO establish a system-build process that guarantees scanner access by default.

Problem Area 2:

The Commission Did Not Apply Patches in a Timely Manner

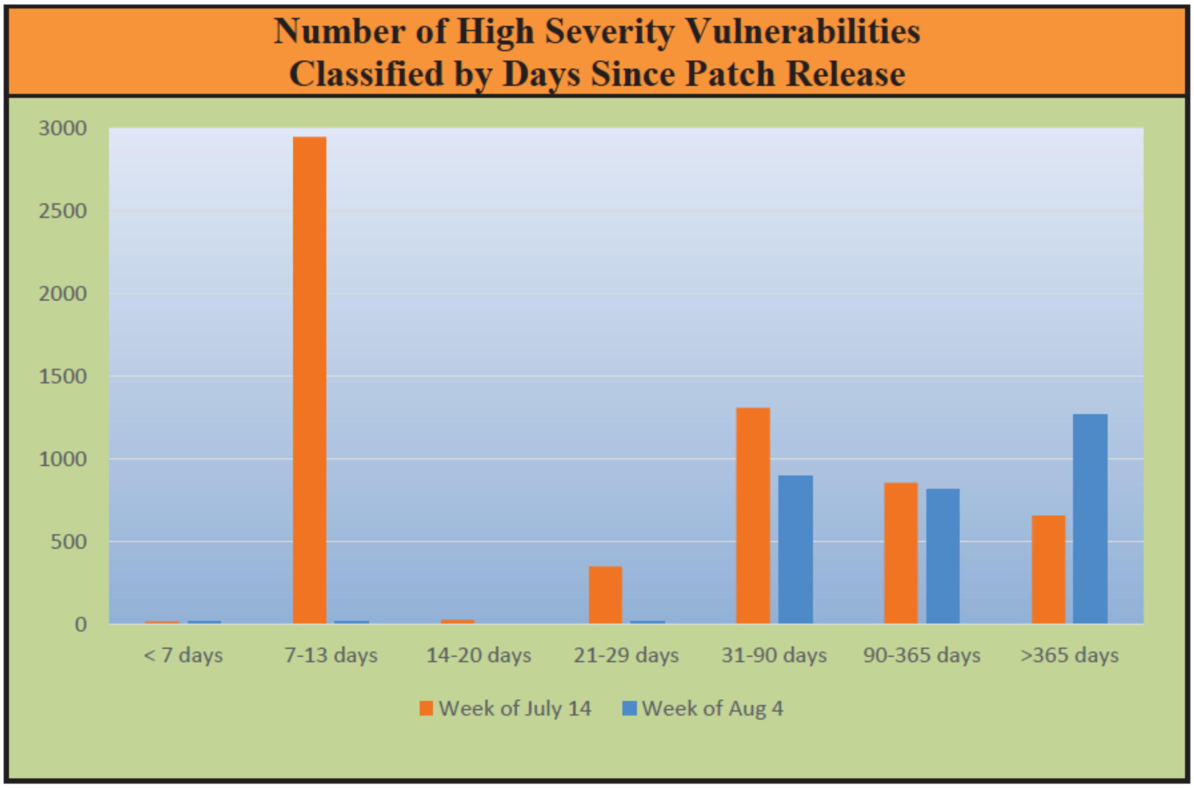
Due to the risk they pose to the network, patches for High severity vulnerabilities should begin to be applied upon patch release. For the purpose of this audit, we rated performance only for the application of released patches addressing High severity vulnerabilities. We did not measure vulnerabilities without a released patch, or any Low or Medium vulnerabilities.

When a vulnerability is publicly acknowledged, each is assigned a risk rating using the Common Vulnerability Scoring System (CVSS). The CVSS score is an industry standard that describes the risk of a specific vulnerability. A CVSS score over 7 indicates a High risk vulnerability. (Scores below 7 indicate Low to Medium-level vulnerabilities)

We found that on average, 2.2% of 438 hosts measured were clean or fully patched. The remaining 97.8% of hosts measured required patches to resolve High severity vulnerabilities.

Many of the missing patches were weeks, months, or years old. Even the anticipated, regularly scheduled monthly Microsoft patches (indicated by the large peak in the 7-13 days section below) were applied when they were more than a week old.

Chart 1: Number of High Severity Vulnerabilities Classified by Days Since Patch Release



This chart also shows that many patches older than 30 days are allowed to persist on the network, in many cases, for years.

These practices place the Commission at risk. There may be a few circumstances when a decision is made not to patch. However, the number of hosts that remain unpatched should be minimized, and the length of time the vulnerabilities persist should be limited.

In one example, the Commission has decided to allow many hosts to remain unpatched to maintain compatibility with a financial system. All of these hosts are at risk, and therefore place the rest of the network at risk. The Commission could choose to minimize the risk theses hosts and its network by fully patching these hosts, and use its existing technology to provide a secure, seamless means of accessing the financial system while maintaining the security of its hosts. It has chosen not to do so, instead leaving these hosts, and therefore the entire network, vulnerable for years.

Recommendation 4: That the Commission patch all High severity application and operating system software vulnerabilities within 48 hours of patch release.

Recommendation 5: That the CIO identify any business needs that require the use of unpatched software and restrict access to a secured thin-client application or other solution that allows user workstations to be fully patched.

Problem Area 3:

The Risk from Missing Patches Was Not Effectively Reported

Patch management reporting is an essential part of the process to quantify the risk for executive management in an easily digestible fashion, so they are able to make informed decisions to manage that risk.

The Commission has published a performance metric, which it calls the Enterprise Vulnerability Index. It uses a complicated formula and describes as its goal any number less than 5. Since only an average of 438 hosts were measured for missing patches, the current metric implies that as long as it doesn't exceed 33 High severity vulnerabilities per host, the Commission will meet its target performance goal to ensure network security.

In previous OIG audits, in order to convey the magnitude of the risk due to missing patches, we have reported on the number of High severity vulnerabilities per host. Another measure sometimes used is to report on the average CVSS score per host. Other than what the Commission has published, we were unable to find any instances where an organization used the log of a sum to describe the security of a network.

The Commission's metric conveys the message to executive management that the Commission has effectively ensured network security. This provides the Commission with a false sense of security, and does not provide actionable information to business owners regarding the risk to the network due to missing patches.

Recommendation 6: That the CIO report on the average number of High severity vulnerabilities per host, or average CVSS score per host, or another score that provides a metric on a per host basis.

Recommendation 7: That the Commission set a goal for missing patches at a number that provides an acceptable level of risk to the Commission.

Management Comments and Our Analysis

On November 5, 2013, Chairman Irving Williamson provided management comments on the draft report. He acknowledged that the Commission did not have an effective process for patching and agreed to make management decisions to address the recommendations in the report.

Objective, Scope and Methodology

Objective:

Is the Commission's process for patching ITCNet systems effective?

Scope:

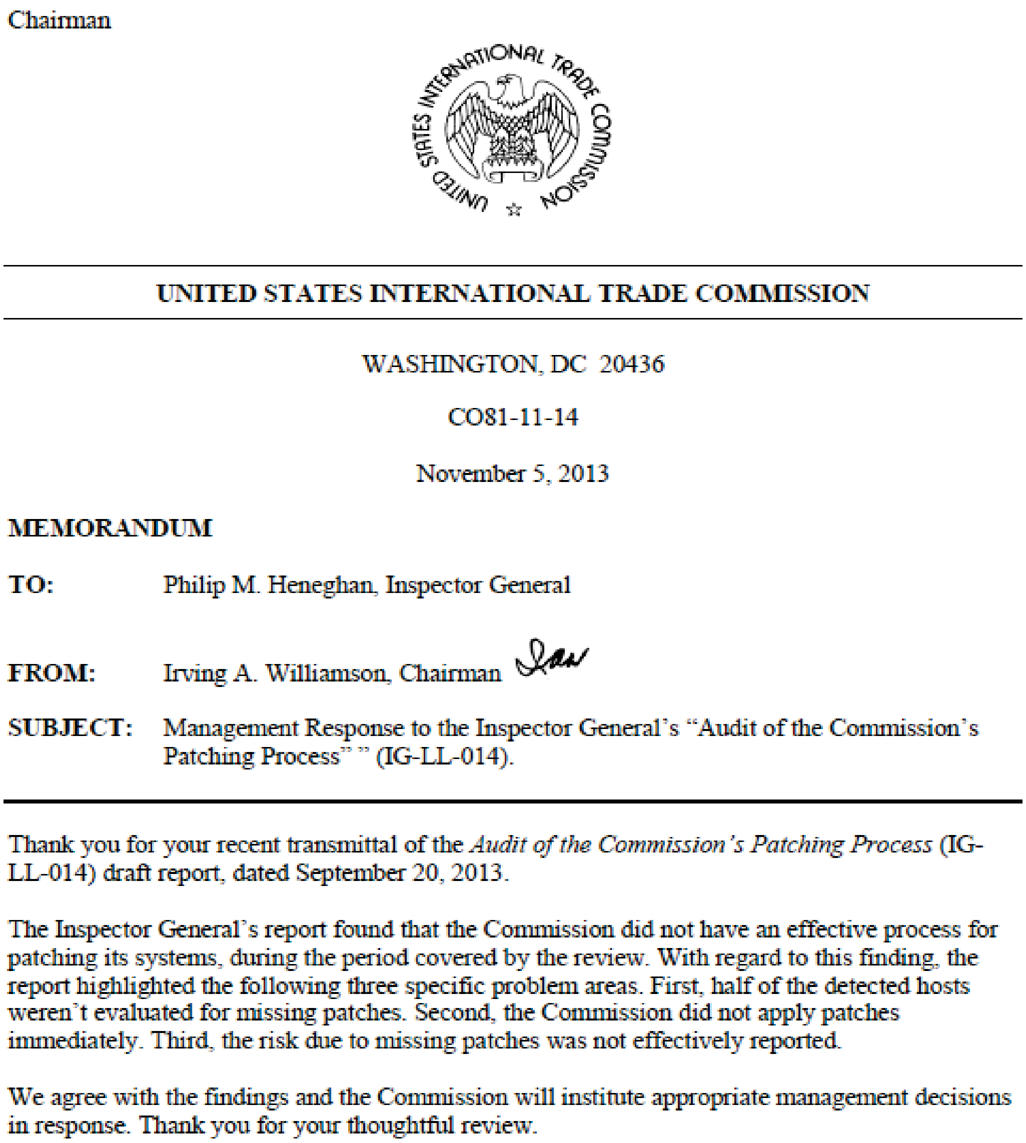
This audit focused on the process for patching systems on ITCNet. To determine the patch-related vulnerability status, we analyzed two sets of scanning data provided by the CIO for the weeks of July 14 and August 8, 2013. This data included all hosts detected as part of the CIO vulnerability management process on the network ranges scanned, including servers, workstations, virtual hosts, and other network equipment providing connectivity and security.

Methodology:

1. Evaluated the risk approach used by the CIO to assess vulnerabilities.
2. We did not scan the network to evaluate patch status, but instead gathered existing vulnerability data from CIO.
3. Identified hosts that were not scanned due to technical or policy issues.
4. Analyzed vulnerabilities to remove false positives, and classified findings to identify trends and the causes of unpatched vulnerabilities.
5. Determined whether patching process was guided by reasonable risk based decisions.
6. Determined whether patch status was being accurately measured.
7. Determined whether patch status was reported to executive management.
8. Determined whether patches were applied in a timely fashion.

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

CO81-11-14

November 5, 2013

MEMORANDUM

TO: Philip M. Heneghan, Inspector General

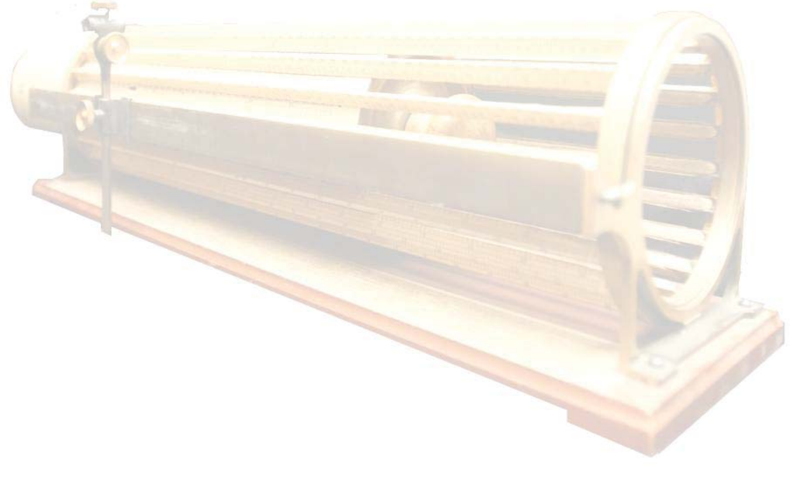
FROM: Irving A. Williamson, Chairman IAW

SUBJECT: Management Response to the Inspector General's "Audit of the Commission's Patching Process" " (IG-LL-014).

Thank you for your recent transmittal of the *Audit of the Commission's Patching Process* (IG-LL-014) draft report, dated September 20, 2013.

The Inspector General's report found that the Commission did not have an effective process for patching its systems, during the period covered by the review. With regard to this finding, the report highlighted the following three specific problem areas. First, half of the detected hosts weren't evaluated for missing patches. Second, the Commission did not apply patches immediately. Third, the risk due to missing patches was not effectively reported.

We agree with the findings and the Commission will institute appropriate management decisions in response. Thank you for your thoughtful review.



"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