Release Notes for the June 25, 2015 SSH Vulnerability Patch for Cisco Content Security Virtual Appliances

First Published: June 25, 2015

Contents

Affected Releases

This patch is required for all virtual appliance releases for email security, web security, and content security management that were downloaded or upgraded before June 25, 2015.

This patch is NOT required for physical hardware appliances or for virtual appliance downloads or upgrades after June 25, 2015.

Fixed Issues

This patch addresses the following PSIRT issue(s):

Title: Multiple Default SSH Keys Vulnerabilities in Cisco Virtual WSA, ESA, and SMA

Cisco Systems, Inc.
www.cisco.com

URL:
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150625-ironport

You can view some details by clicking the link to view bug information in the Cisco Bug Search Tool.

Bug	Description
CSCuu95676	Virtual ESA not generating new SSH HostKey post deployment
CSCuu95994	Virtual ESA: preinstalled keys allow remote root access without customer's consent
CSCus29681	Virtual WSA not generating new SSH HostKey post deployment
CSCuu95988	Virtual WSA: preinstalled keys allow remote root access without customer's consent
CSCuu96601	Virtual SMA not generating new SSH HostKey post deployment
CSCuu96630	Virtual SMA: preinstalled keys allow remote root access without customer's consent

Installation Instructions

Before Installation

Before installing the patch, perform any pre-upgrade tasks that are documented in the release notes and online help or user guide for your release(s).

The appliance will prompt you to reboot after installing the patch. This reboot is required.

This patch should take only a few minutes to install.

If you are updating a Security Management appliance:

- You will need appropriate credentials for managed appliances in order to re-establish connection to those appliances after installation.
- If you use centralized configuration management for Web Security appliances, you will need to reassign the configuration master to each appliance after installing the patch. Suggestion: Before you install the patch, take a screen shot of the list on the Web > Utilities > Configuration Masters > Edit Appliance Assignment List page.

Installing the Patch

Instructions:

- You must use the command-line interface (CLI) to install this patch. Do NOT use the web interface to install this patch, even if you see this patch among the upgrade options.
- Use the `upgrade` command and select `cisco-sa-20150625-ironport SSH Keys Vulnerability Fix`.
- For email and management appliances (ESA and SMA), if `downloadinstall` is available as an `upgrade` option on your release, you MUST use it. The `download` option does not work for this patch.
- If you are installing the patch on SMA 8.4.0-150, see required actions at Known Issues, page 5.

Sample transcript for appliances with the `downloadinstall` option:

```
esa> upgrade
Choose the operation you want to perform:
- DOWNLOADINSTALL - Downloads and installs the upgrade image (needs reboot).
- DOWNLOAD - Downloads the upgrade image.
[]> downloadinstall

Upgrades available.
1. cisco-sa-20150625-ironport SSH Keys Vulnerability Fix
[]> 1

Would you like to save the current configuration to the configuration directory before
upgrading? [Y]>

Would you like to email the current configuration before upgrading? [N]>

Do you want to include passwords? Please be aware that a configuration without passwords
will fail when reloaded with loadconfig. [Y]>

Performing an upgrade may require a reboot of the system after the upgrade is applied.
You may log in again after this is done. Do you wish to proceed with the upgrade? [Y]>

Checking if 'Cisco-Ironport SSH Keys Vulnerability' patch is required
'Cisco-Ironport SSH Keys Vulnerability' patch is required
'Cisco-Ironport SSH Keys Vulnerability' patch applied

Upgrade will be complete after this mandatory reboot.

Upgrade installation finished.
Enter the number of seconds to wait before forcibly closing connections.
[30]>
```

Press <Enter>.

The appliance will reboot after the specified number of seconds.

Sample transcript for appliances without multiple upgrade options:

```
wsa > upgrade

Upgrades available.
1. cisco-sa-20150625-ironport SSH Keys Vulnerability Fix
[1]> 1

Would you like to save the current configuration to the configuration directory before
upgrading?
[Y]> n
```

```
Would you like to email the current configuration before upgrading?
[N]>

Performing an upgrade may require a reboot of the system after the upgrade is applied.
You may log in again after this is done. Do you wish to proceed with the upgrade?
[Y]>

Checking if 'Cisco-Ironport SSH Keys Vulnerability' patch is required
'Cisco-Ironport SSH Keys Vulnerability' patch is required
'Cisco-Ironport SSH Keys Vulnerability' patch applied

Upgrade will be complete after this mandatory reboot.

Upgrade installation finished.

Reboot takes about 20 minutes to complete. Do not interrupt power to the appliance during
this time.
Are you sure you want to reboot?
[N]> y

System shutting down. Please wait while the system services are stopped...Connection to
<your wsa> closed by remote host.
Connection to <your wsa> closed.
```

The appliance will now reboot.

After Installation

After installing the patch:

- Perform all of the activities you would normally do after an upgrade. See the release notes and the online help or user guide for your release.
- Remove the existing entry for your appliance from the known hosts list in your ssh utility. Then ssh to the appliance and accept the connection with the new key.
- If you use SCP push to transfer logs to a remote server (including Splunk): Clear the old SSH host key for the appliance from the remote server.
- On Security Management appliances:
  - Use the `logconfig > hostkeyconfig > delete` CLI command as many times as needed to clear the old key associated with each managed ESA and WSA virtual appliance.
  - Re-establish the connection to each managed appliance and (if applicable) reassign each managed appliance to the appropriate configuration master:

    1. Go to Management Appliance > Centralized Services > Security Appliances and click the link for an appliance in the list.

    2. Click Establish Connection.

3. (Managed WSAs only) If your appliance is configured for centralized configuration management, re-assign the Configuration Master to each managed WSA.

4. Submit and commit your changes if applicable.

5. Repeat for each managed appliance.

- For cluster configurations (Email Security appliances):
  - Delete the host keys of all virtual Email Security appliances using `logconfig > hostkeyconfig > delete` (The host keys are modified after upgrade.)
  - Add the new key for each virtual Email Security appliance to all machines in the cluster using `logconfig > hostkeyconfig > scan`. Use the IP address of each virtual Email Security appliance in the cluster.

    For example, if there are two virtual Email Security appliances in a cluster, update the host keys of both appliances on both machines.

    So, run the following commands on both appliances in the cluster:
    `logconfig > hostkeyconfig > scan > <IP address of vESA1>`
    and
    `logconfig > hostkeyconfig > scan > <IP address of vESA2>`.
  - Reconnect the machines to the cluster using `clusterconfig` command.
  - Verify that the machines are reconnected properly by using the `clusterconfig > connstatus` command to check connection status.

Known Issues

If you are installing the patch on SMA 8.4.0-150:

You will see an "Upgrade failure" message after running the upgrade, but the patch has installed correctly. However, you must reboot the appliance manually to complete the installation process:

After you see "Upgrade failure," the `upgrade` command options will reappear. Press <Enter> to exit the `upgrade` command, then enter the `reboot` command.

You should also receive an alert about an application fault; ignore this.

Related Documentation

In addition to the main documentation in the following table, information about other resources, including the knowledge base and Cisco support community, is in the More Information chapter in the online help and User Guide PDF.

Documentation For Cisco Content Security Products:	Is Located At:
Security Management appliances	http://www.cisco.com/c/en/us/support/security/content-security-management-appliance/tsd-products-support-series-home.html
Web Security appliances	http://www.cisco.com/c/en/us/support/security/web-security-appliance/tsd-products-support-series-home.html

Documentation For Cisco Content Security Products:	Is Located At:
Email Security appliances	http://www.cisco.com/c/en/us/support/security/email-security-appliance/tsd-products-support-series-home.html
Command Line Reference guide for content security products	http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-command-reference-list.html
Cisco Email Encryption	http://www.cisco.com/c/en/us/support/security/email-encryption/tsd-products-support-series-home.html

Service and Support

International: Visit http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

Support Site: Visit http://www.cisco.com/web/services/acquisitions/ironport.html

For non-critical issues, you can also access customer support from the appliance. For instructions, see the User Guide or online help.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.