Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco ISR 4000 Series Routers

First Published: 2020-02-28

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco ISR 4000 Series Routers

This document provides instructions on how to address the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco ISR 4000 Series Routers.

Note Cisco recommends upgrading Field Programmable Gate Arrays (FPGA) as a solution for the Cisco Secure Boot Hardware Tampering Vulnerability. For more details of the vulnerability and affected products, refer to https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot.

Prerequisites for Upgrading FPGA (CPLD)

Download the image from the CCO website and copy it to USB or bootflash of the router which is scheduled for the upgrade.

Table 1: CPLD Versions and Images

Platforms	CPLD Version	CCO URL for the CPLD Image
ISR4461	19051340	CPLD Update Tool_isr_4400v2_cpld_update_v2.0.SPA.bin
ISR4451	19042950	CPLD Update Tool_isr4400_cpld_update_v2.0.SPA.bin
ISR4431	19042950	CPLD Update Tool_isr4400_cpld_update_v2.0.SPA.bin
ISR4351	19040541	CPLD Update Tool_isr4300_cpld_update_v2.0.SPA.bin
ISR4331	19040541	CPLD Update Tool_isr4300_cpld_update_v2.0.SPA.bin

Platforms	CPLD Version	CCO URL for the CPLD Image
ISR4321	19040541	CPLD Update Tool_isr4300_cpld_update_v2.0.SPA.bin
ISR4221	19042420	CPLD Update Tool_isr4200_cpld_update_v2.0.SPA.bin

Note Do not perform any power cycle or remove the power cable during the CPLD update. If there is a power loss during the update, it may result in corruption of the boot image and it may require RMA of the equipment.

Upgrading CPLD

You can upgrade the CPLD using two different methods:

- Upgrading from Rommon Prompt (OR)
- Upgrading from IOS SSH/VTY Prompt

Upgrading from Rommon Prompt

To upgrade from Rommon prompt, you require the console access. This procedure is described in Updating CPLD form Rommon Prompt section. Since it takes only a few steps to complet the upgrade, it is recommended to use this procedure. Also, the update utility is launched directly from Rommon prompt which facilitates detection and recovery if there are any issues encountered by the utility.

Upgrading from IOS SSH/VTY Prompt

This procedure is performed only from IOS SSH/VTY prompt. This procedure is described in Updating CPLD from IOS SSH/VTY Prompt section. You can use the IOS SSH/VTY prompt only when you do not have access to console which prevents launching the upgrade utility directly from the Rommon.

For upgrading the system, select the appropriate method based on the console access.

Updating CPLD from Rommon Prompt

To upgrade CPLD, run the upgrade utility image:

Procedure

Step 1 Copy the utility to USB or to bootflash: using FTP or TFTP.

Step 2 Save the current running configurations and backup it to bootflash.

```
Router#copy running-config bootflash:running-config_24jan2020
Destination filename [running-config_24jan2020]?
6222 bytes copied in 0.536 secs (11608 bytes/sec)
Router#

Router#copy run start
Building configuration...
```

```
[OK]
Router#
```

Step 3 Change the configuration register to 0x0.

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#config-register 0x0
Router(config)#end
Router#copy run start
```

Step 4 Issue the router reload command and ensure that the Rommon prompt is displayed on the router.

```
Router#reload
```

Step 5 Initiate the upgrade using the following CLI, and follow the instructions from the tool.

Note If the image is copied in USB, execute the following command:

```
boot usb0:isr4400_cpld_update_v2.0_SPA.bin
```

If the image is copied in Bootflash, execute the following command:

```
boot bootflash:isr4400_cpld_update_v2.0_SPA.bin
```

```
rommon 2 > boot bootflash:isr4400_cpld_update_v2.0_SPA.bin


Package header rev 1 structure detected
IsoSize = 0
Calculating SHA-1 hash...Validate package: SHA-1 hash:
 calculated 53D10090:FFB242CF:831A6271:41ABD240:234332FA
 expected   53D10090:FFB242CF:831A6271:41ABD240:234332FA
RSA Signed RELEASE Image Signature Verification Successful.
Image validated


    Cisco ISR4400 CPLD Programming Utility

  ****************************************
  **                                    **
  **     DO NOT TURN OFF THE POWER OR     **
  **   RESET THE BOX DURING THE UPGRADE   **
  **                                    **
  ****************************************

Detected platform: ISR4451
CPLD version: 16092742
The CPLD is unlocked.


Erasing CPLD image ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
Programming CPLD image ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
Verifying CPLD image ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
CPLD image verified correctly !!

 *** DONE ***
```

```
Power cycling the platform ...
                              ********************************
```

The following message confirms the upgrade is successful:

CPLD image verified correctly !!

In this case, skip **Step 6** and **Step 7**, and proceed to **Step 8** for verification.

Step 6 If the Upgrade is not successful, the following message appears: *CPLD image failed to verify correctly !!*

Important Do not power cycle the platform.

Retry the CPLD update by repeating **Step 5**.

Step 7 After the retry, if the upgrade still fails, reach out to Cisco TAC for further assistance.

Step 8 After the upgrade is complete, device power cycles automatically, and the rommon prompt is displayed to boot the IOS image.

```
Sample IOS boot steps are:

rommon 1 > dir bootflash:

0   621353159 -rw-     isr4400-universalk9.16.10.01.SPA.bin

rommon 2 > boot bootflash:isr4400-universalk9.16.10.01.SPA.bin
```

Updating CPLD from IOS SSH/VTY Prompt

You can update the CPLD from the IOS SSH/VTY prompt when you do not have acces to the console. If you have access to the console, follow the steps provided in Updating CPLD from Rommon Prompt section. To update CPLD without console access, run the update utility image through boot system mechanism:

Note When you upgrade the CPLD version due to Cisco secure boot hardware tampering vulnerability from IOS SSH/VTY in the Cisco 4000 Series router with rommon version IOS XE 15.X, the router will go into an endless bootloop that require console connection to recover the router. To avoid this endless bootloop, before upgrading the CPLD version, upgrade the rommon version to 16.2(1r) or higher.

Procedure

Step 1 Copy the utility to USB or to bootflash: using FTP or TFTP.

Step 2 Save the current running configurations and backup it to bootflash.

```
Router#copy running-config bootflash:running-config_24jan2020
Destination filename [running-config_24jan2020]?
6214 bytes copied in 0.438 secs (14187 bytes/sec)
Router#
```

Step 3 Update the boot system image list to include the utility as the **first** image in the list, followed by the current IOS image0.

Display the current *boot system* image list:

```
Router#show run | inc boot
boot-start-marker
boot system bootflash: isr4300-universalk9.16.11.02.SPA.bin
boot-end-marker
Router#
```

Remove all IOS images from the *boot system* image list:

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#no boot system
Router(config)#
```

Add the utility as the first entry in the *boot system* image list:

```
Router(config)#boot system flash bootflash:isr4300_cpld_update_v2.0.SPA.bin
```

Add the previously removed IOS image as the second entry in the *boot system* image list:

```
Router(config)# boot system flash bootflash: isr4300-universalk9.16.11.02.SPA.bin
Router(config)#end
```

Verify that the *boot system* image list is correct, with the utility as the first entry and the IOS image as the second entry:

```
Router#show run | inc boot
boot-start-marker
boot system flash bootflash:isr4300_cpld_update_v2.0.SPA.bin
boot system flash bootflash: isr4300-universalk9.16.11.02.SPA.bin
boot-end-marker
Router#
```

Step 4 Verify that the BOOT ROMMON variable matches the *boot system* image list.

```
Router# show romvar | inc BOOT

BOOT =
bootflash:isr4300_cpld_update_v2.0.SPA.bin,1;bootflash:isr4300-universalk.16.11.02.SPA.bin,1;
```

Step 5 Save the updated running-config to the startup-config.

```
Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

Step 6 Initiate the upgrade by issuing the **reload** command.

Important Since the upgrade is being performed from IOS console, the utility will run silently. There will be no console output as shown in the previous Updating CPLD section.

```
Router#reload
Proceed with reload? [confirm]

*Jan 27 20:24:07.428: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
Command.
```

Step 7 Wait for system to complete CPLD upgrade and automatically reload the device (This process may take approximately 10 minutes). During this time:

```
The utility will automatically perform the CPLD upgrade.

When the CPLD upgrade is complete, the utility will automatically power-cycle the device
and advance to the second image in the configured 'boot system' image list.

The system will continue booting and initialize normally. Wait for 10 minutes for CPLD
upgrade and system boot to complete before attempting to login.
```

Step 8 Login to the system and verify the CPLD is updated correctly.

```
Router#show hw-programmable 0
Hw-programmable versions

Slot              CPLD version              FPGA version
------------------------------------------------------------
0                 19040541                  N/A
```

Note Verify the CPLD version with the platforms given in table *CPLD Versions and Images*.

Step 9 If the CPLD upgrade fails, contact Cisco TAC for further assistance.

Important Do not power cycle the platform.

Step 10 Remove the utility from the boot system image list.

```
Router(config)#no boot system flash bootflash:isr4300_cpld_update_v2.0.SPA.bin
```

*Verify the utility has been removed from the 'boot system' image list, and the IOS image is now the **first** entry:*

```
Router#show run | inc boot
boot-start-marker
boot system flash bootflash: isr4300-universalk9.16.11.02.SPA.bin
boot-end-marker
Router#
```

Note This step removes the utility from the boot system image list to avoid subsequent invocations of the utility when system is reloaded. There is no harm in running the utility multiple times but it introduces a delay while the utility determines if the upgrade is already performed. Also, it requires additional power-cycle.

Step 11 Verify that the BOOT ROMMON variable matches the boot system image list.

```
Router# show romvar | inc BOOT
BOOT = bootflash:isr4300-universalk9.16.11.02.SPA.bin,1;
```

Step 12 Save the updated running-config to the startup-config.

```
Router#copy run start
Destination filename [startup-config]?
Building configuration...
[OK]
Router#
```

Verifying CPLD Update

To verify the CPLD upgrade, use the following command:

```
Router#show hw-programmable 0
Hw-programmable versions

Slot              CPLD version              FPGA version
--------------------------------------------------------
0                 19042950                  N/A
```

Note Verify the CPLD version with the platforms given in table *CPLD Versions and Images*