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

First Published: 2019-08-06

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.

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.

Note The following procedure requires access to the console port on the router. It must be performed either locally or remotely with out-of-band access.

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: FPGA Versions and Images

Platforms	FPGA Version	CCO URL for the FPGA Image
ISR4461	19051340	CPLD Update Tool isr4400v2_cpld_update_v1.1_SPA.bin

Platforms	FPGA Version	CCO URL for the FPGA Image
ISR4451/ISR4431	19042950	CPLD Update Tool isr4400_cpld_update_v1.1_SPA.bin CPLD Update Tool isr4400_cpld_update_v1.1_SPA.bin
ISR4351/ISR4331/ISR4321	19040541	CPLD Update Tool isr4300_cpld_update_v1.1_SPA.bin CPLD Update Tool isr4300_cpld_update_v1.1_SPA.bin CPLD Update Tool isr4300_cpld_update_v1.1_SPA.bin
ISR4221	19042420	isr4200_cpld_update_v1.1_SPA.bin

Upgrading CPLD

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_15may2019
Destination filename [running-config_15may2019]?
6222 bytes copied in 0.536 secs (11608 bytes/sec)
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_v1.1_SPA.bin
```

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

```
boot usb0:isr4400_cpld_update_v1.1_SPA.bin
```

```
rommon 2 > boot bootflash:isr4400_cpld_update_v1.1_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
```

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 *FPGA Versions and Images*