Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-40 Wireless Controller

This chapter provides instructions on how to address the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-40 Wireless Controller.

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 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot.

Prerequisites for Upgrading FPGA

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

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

Upgrading FPGA

To upgrade FPGA, run the upgrade utility image:

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.

```
WLC#copy running-config bootflash:running-config_15may2019
Destination filename [running-config_15may2019]?
6222 bytes copied in 0.536 secs (11608 bytes/sec)
WLC#

WLC#write  memory
Building configuration...
[OK]
WLC#
```

Step 3 Note down the configuration register value and change it to 0x0.

```
WLC#sh ver | in Configuration
Configuration register is 0x2102
WLC#


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

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

```
WLC#reload


System configuration has been modified. Save? [yes/no]: yes
Building configuration...
[OK]
```

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:C9800-40_fpga_prog.16.0.0.xe.bin
```

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

```
boot bootflash:C9800-40_fpga_prog.16.0.0.xe.bin
```

```
rommon 2 > boot bootflash:C9800-40_fpga_prog.16.0.0.xe.bin
File size is 0x015a3814
Located C9800-40_fpga_prog.16.0.0.xe.bin
Image size 22689808 inode num 32, bks cnt 5540 blk size 8*512
################################################################################################################################################################################################################

Boot image size = 22689808 (0x15a3810) bytes


ROM:RSA Self Test Passed
ROM:Sha512 Self Test Passed

Package header rev 1 structure detected
Calculating SHA-1 hash...done
validate_package_cs: SHA-1 hash:
        calculated 9b991366:34fd025f:987b920f:934aa266:fc2e0d08
        expected   9b991366:34fd025f:987b920f:934aa266:fc2e0d08
Validating main package signatures

RSA Signed RELEASE Image Signature Verification Successful.
```

```
Image validated

    Cisco ASR1K FPGA Programming Utility

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

  Press 'Y' or 'y' to upgrade
  or any other key to reboot

Detected Board Type: CE9800-40

SPI Flash Device ID: 009d6016

Programming Flash ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
Verifying Flash ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
FPGA image verified correctly !!

Router Power Cycle is needed for the changes to take effect

Press a key to Power cycle ...

Power cycling the box ...


  à

Initializing Hardware ...

System integrity status: 90170400 12030106
U

System Bootstrap, Version 16.9(4r), RELEASE SOFTWARE
Copyright (c) 1994-2018  by cisco Systems, Inc.

Current image running: Boot ROM1
Last reset cause: PowerOn
```

Important **********

The following message confirms the upgrade is successful:

FPGA 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: *FPGA image failed to verify correctly !!*

Retry the upgrade by issuing **Yes**.

```
Use can issue "y" or "Y" to retry.
```

```
Detected Board Type: CE9800-40
SPI Flash Device ID: 00202015

Programming Flash ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
Verifying Flash ...
|.......|.......|.......|.......|.......|.......|.......|.......|

FPGA image failed to verify correctly !!

Upgrade failed. Retrying ...

       Cisco ASR1K FPGA Programming Utility

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

  Press 'Y' or 'y' to upgrade
  or any other key to reboot

Detected Board Type: CE9800-40

SPI Flash Device ID: 00202015

Programming Flash ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
Verifying Flash ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
FPGA image verified correctly !!

Router Power Cycle is needed for the changes to take effect

Press a key to Power cycle ...

Power cycling the box ...

ýü

Initializing Hardware ...

System integrity status: 90170400 12030106

U

System Bootstrap, Version 16.3(2r), RELEASE SOFTWARE
Copyright (c) 1994-2016  by cisco Systems, Inc.

Current image running: Boot ROM0

Last reset cause: CPU-ResetRequest


rommon 1 >
```

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

Step 8 Once 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:
File System: EXT2/EXT3

15         526240224 -rw-r--r--     C9800-universalk9_wlc.2019-04-25_13.46_vgothe.SSA.bin

rommon 2 > boot bootflash: C9800-universalk9_wlc.2019-04-25_13.46_vgothe.SSA.bin
```

Step 9 Revert back the configuration register value to its original value.

```
WLC#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
WLC(config)#config-register 0x2102
WLC(config)#end
WLC#write
```

Verifying FPGA Upgrade

To verify the FPGA upgrade, use the following command:

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

Slot              CPLD version              FPGA version
------------------------------------------------------------
0                 19030712                   N/A
```