Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

First Published: 2019-05-17

CONTENTS

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

iii

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

iv

Preface

This preface describes this guide and provides information about the conventions used in this guide, along with details about related documentation. It includes the following sections:

Document Revision History

The following table shows the changes made to this document:

Date	Change Summary
May 2018	First version of the document.

Document Objectives

This publication describes the instructions for addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller.

Audience

This publication is primarily a field notice for addresing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller.

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

v

Conventions

Text Type	Indication
User input	Text the user should enter exactly as shown or keys a user should press appear in this font.
Document titles	Document titles appear in *this font*.
System output	Terminal sessions and information that the system displays appear in **this font**.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
String	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
! #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

vi

□ **Timesaver**: Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Documentation

See the following documentation for more information about the Cisco Catalyst 9800-80 Wireless Controller:

- *Release Notes for Cisco Catalyst 9800 Wireless Controller Cisco Catalyst 9800-80 Wireless Controller*

- *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*

- *Cisco Catalyst 9800 Series Wireless Controller Command Reference*

- *Cisco Wireless Solutions Software Compatibility Matrix*

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation.

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

vii

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

viii

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

This chapter provides instructions on how to address the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 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.

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

1

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

Upgrading FPGA

```
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:C9800-80_fpga_prog.16.0.0.xe.bin
> ```
>
> If the image is copied in Bootflash, execute the following command:
>
> ```
> boot bootflash:C9800-80_fpga_prog.16.0.0.xe.bin
> ```

```
rommon 1 > boot usb0:C9800-80_fpga_prog.16.0.0.xe.bin
Located C9800-80_fpga_prog.16.0.0.xe.bin, start cluster is 786864

##################################################################################################################################
Image loaded
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
```

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

2

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

Upgrading FPGA

```
    Cisco ASR1K FPGA Programming Utility

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

<mark>**Press 'Y' or 'y' to upgrade**
or any other key to reboot</mark>

```
Detected Board Type: CE9800-80

SPI Flash Device ID: 0020ba17

Programming Flash ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
Verifying Flash ...
|.......|.......|.......|.......|.......|.......|.......|.......|
################################################################
```
<mark>FPGA image verified correctly !!</mark>

```
Router Power Cycle is needed for the changes to take effect

Press a key to Power cycle ...

Power cycling the box ...


    R.

Initializing Hardware ...

System integrity status: 90170200 12030106


System Bootstrap, Version 16.10(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018  by cisco Systems, Inc.

Current image running: Boot ROM0
Last reset cause: PowerOn

C9800-80-K9 platform with 67108864 Kbytes of main memory
```

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.
```

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

3

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

Upgrading FPGA

```
Detected Board Type: CE9800-80
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: CE9800-80

SPI Flash Device ID: 0020ba17

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 ...

R

Initializing Hardware ...

System integrity status: 90170200 12030106

U

System Bootstrap, Version 16.10(3r), RELEASE SOFTWARE
Copyright (c) 1994-2018  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.

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

4

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

Verifying FPGA Upgrade

```
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
```

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

5

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

Verifying FPGA Upgrade

Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-80 Wireless Controller

6