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

First Published: 2019-05-15

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB’s public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

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 9800-40 Wireless Controller.

Audience

This publication is primarily a field notice for addresing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco Catalyst 9800-40 Wireless Controller.

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.

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

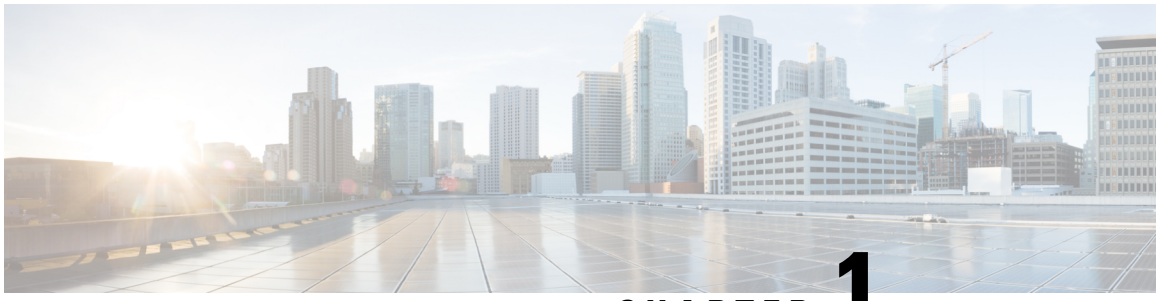
See the following documentation for more information about the Cisco Catalyst 9800-40 Wireless Controller:

- *Release Notes for Cisco Catalyst 9800 Wireless Controller Cisco Catalyst 9800-40 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.



CHAPTER 1

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
```