Cisco Nexus 9000 Series NX-OS Mode Switch FPGA/EPLD Upgrade Release Notes, Release 10.3(1)

© 2022 – 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

This document lists the current and past versions of EPLD images and describes how to update them for use with the Cisco Nexus 9000 Series switches.

This document also covers later releases. If a new Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes document isn't available, then that means that these are the latest available numbers for upgrade.

The table lists the changes to this document.

Table 1. Changes to this Document

Date	Description
August 19, 2022	Release 10.3(1) became available.
June 3, 2024	Updates to Table 3 Cisco Nexus 93240YC-FX2 (N9K-C93240YC-FX2) values.
November 9 2024	Enhanced and moved Secure Boot content to rear of document. Updated command to **install epld bootflash:<image-name> module all** and **install epld bootflash:<image-name> module all golden** in Nexus 9000 TOR section.

Introduction

The Cisco Nexus 9000 Series NX-OS mode switches contain several programmable logical devices (PLDs) that provide hardware functionalities in all modules. Cisco provides electronic programmable logic device (EPLD) image upgrades to enhance hardware functionality or to resolve known issues. PLDs include electronic programmable logic devices (EPLDs), field programmable gate arrays (FPGAs), and complex programmable logic devices (CPLDs), but they do not include ASICs. In this document, the term EPLD is used for FPGA and CPLDs.

The advantage of having EPLDs for some module functions is that when you need to upgrade those functions, you just upgrade their software images instead of replacing their hardware.

Note: EPLD image upgrades for a line card disrupt the traffic going through the module because the module must power down briefly during the upgrade. The system performs EPLD upgrades on one module at a time, so at any one time the upgrade disrupts only the traffic going through one module.

Cisco provides the latest EPLD images with each release. Typically, these images are the same as provided in earlier releases but occasionally some of these images are updated. These EPLD image updates are not mandatory unless otherwise specified. The EPLD image upgrades are independent from the Cisco In Service Software Upgrade (ISSU) process, which upgrades the system image with no impact on the network environment.

When Cisco makes an EPLD image upgrade available, these release notes announce their availability, and you can download the EPLD images from https://software.cisco.com/download/navigator.html.

When choosing an EPLD version for upgrade, ensure you have already installed the corresponding NXOS software version first. It is generally not supported to upgrade to a newer EPLD image built for a future version of NXOS while running on an older NXOS version, unless explicitly supported as per the specific EPLD Release Notes. NXOS and EPLD images are labeled for their related version to avoid any unsupported upgrades.

© 2022 – 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

When to Upgrade EPLDs

When new EPLD images are available, the upgrades are always recommended if your network environment allows for a maintenance period in which some level of traffic disruption is acceptable. If such a disruption is not acceptable, then consider postponing the upgrade until a better time.

Note: The EPLD upgrade operation is a disruptive operation. Execute this operation only at a programmed maintenance time. The system ISSU upgrade is a nondisruptive upgrade.

Note: Do not perform an EPLD upgrade during an ISSU system upgrade.

Note: EPLD version is backward compatible.

Switch Requirements

- The Cisco Nexus 9000 Series switch must be running the Cisco NX-OS operating system
- You must be able to access the switch through a console, SSH, or Telnet (required for setting up a switch running in NX-OS mode).
- You must have administrator privileges to work with the Cisco Nexus 9000 Series switch.

EPLD Upgrades Available for NX-OS Mode Releases 10.1(2) through 10.3(1)

Each EPLD image that you can download from Software Download page is a bundle of EPLD upgrades packaged into a single EPLD image file. To see the available EPLD versions for the Nexus 9000 standalone and module switches on this release, see the tables.

Note: All updates to an image are shown in boldface. If more than one release is shown for a column, the boldface applies to the first release listed for the column.

Note: This release of EPLD addresses the Secure Boot Hardware Tampering vulnerability for Nexus 9000 Series switches. Please refer to this Security Advisory for more information - https://www.cisco.com/c/en/us/support/docs/csa/cisco-sa-20190513-secureboot.html.

Table 2. Available EPLD Images for the Cisco Nexus 9200, 9300, 9300-EX, and 9300-FX Platform Switches

Switch or Uplink Module	EPLD Device	Release 10.1(2)	Release 10.2(1)	Release 10.2(2)	Release 10.2(3)	Release 10.3(1)
Cisco Nexus 92348GC-X (N9K-C92348GC-X)	IOFPGA	0x14 (0.020)	0x14 (0.020)	0x14 (0.020)	0x14 (0.020)	0X14 (0.020)
Cisco Nexus 93108TC-EX (N9K-C93108TC-EX)	IOFPGA	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)
	MIFPGA	0x2 (0.002)	0x2 (0.002)	0x2 (0.002)	0x2 (0.002)	0x2 (0.002)
Cisco Nexus 93108TC-FX (N9K-C93108TC-FX)	IOFPGA	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)
	MIFPGA	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)
Cisco Nexus 93108TC2-FX (N9K-C93108TC2-FX)	IOFPGA	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)
	MIFPGA	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Switch or Uplink Module	EPLD Device	Release 10.1(2)	Release 10.2(1)	Release 10.2(2)	Release 10.2(3)	Release 10.3(1)
Cisco Nexus 9316D-GX (N9K-C9316D-GX)	IOFPGA	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	0x18 (0.024)
	MIFPGA	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)
Cisco Nexus 93180YC-FX3 (N9K-C93180YC-FX3)	IOFPGA	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)
	MIFPGA	0x15 (0.021)	0x15 (0.021)	0x16 (0.022)	**0x18 (0.024)**	0x18 (0.024)
Cisco Nexus 93180YC-FX3S (N9K-C93180YC-FX3S)	IOFPGA	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)
	MIFPGA	0x15 (0.021)	0x15 (0.021)	0x15 (0.022)	**0x17 (0.023)**	0x17 (0.023)
Cisco Nexus 93180YC-FX3H (N9K-C93180YC-FX3H)	IOFPGA	NA	NA	NA	NA	**0x12 (0.018)**
	MIFPGA	NA	NA	NA	NA	**0x18 (0.024)**
Cisco Nexus 93180YC-EX (N9K-C93180YC-EX)	IOFPGA	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)
	MIFPGA	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)
Cisco Nexus 93180YC-FX (N9K-C93180YC-FX)	IOFPGA	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)
	MIFPGA	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)
Cisco Nexus 93216TC-FX2 (N9K-C93216TC-FX2)	IOFPGA	0x16 (0.022)	0x16 (0.022)	0x16 (0.022)	0x16 (0.022)	0x16 (0.022)
	MIFPGA0	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)
	MIFPGA1	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)
Cisco Nexus 93240YC-FX2 (N9K-C93240YC-FX2)	IOFPGA	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	**0x16 (0.022)**
	MIFPGA1	0x8 (0.007)	0x8 (0.007)	0x8 (0.007)	0x8 (0.007)	0x8 (0.007)
	MIFPGA2	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)
Cisco Nexus 9332C (N9K-C9332C)	IOFPGA	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	**0x16 (0.022)**
	MIFPGA	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)
Cisco Nexus 9332D-GX2B (N9K-C9332D-GX2B)	IOFPGA	N/A	N/A	0x11 (0.017)	0x11 (0.017)	**0x12 (0.018)**
	MIFPGA	N/A	N/A	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)
Cisco Nexus 9336C-FX2 (N9K-C9336C-FX2)	IOFPGA	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	**0x16 (0.022)**
	MIFPGA	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)
Cisco Nexus 9336C-FX2-E (N9K-C9336C-FX2-E)	IOFPGA	**0x10 (0.016)**	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	**0x12 (0.018)**
	MIFPGA	0x4 (0.004)	**0x5 (0.005)**	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)
Cisco Nexus 93360YC-FX2	IOFPGA	0x16 (0.022)	0x16 (0.022)	0x16 (0.022)	0x16 (0.022)	0x16 (0.022)

© 2022 – 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Switch or Uplink Module	EPLD Device	Release 10.1(2)	Release 10.2(1)	Release 10.2(2)	Release 10.2(3)	Release 10.3(1)
(N9K-C93360YC-FX2)	MIFPGA0	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)
	MIFPGA1	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)
Cisco Nexus 9348GC-FXP (N9K-C9348GC-FXP)	IOFPGA	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)
	MIFPGA	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)
Cisco Nexus 9348GC-FXP (N9K-C9348GC2-FXP)	IOFPGA	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)
	MIFPGA	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)
Cisco Nexus 93600CD-GX (N9K-C93600CD-GX)	IOFPGA	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	**0x18 (0.024)**
	MIFPGA	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)
Cisco Nexus 9364C (N9K-C9364C)	IOFPGA	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)
	MIFPGA0	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)
	MIFPGA1	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)
Cisco Nexus 9364C-GX (N9K-C9364C-GX)	IOFPGA	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)
	MIFPGA0	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)
	MIFPGA1	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)
Cisco Nexus 9364D-GX2A (N9K-C9364D-GX2A)	IOFPGA	N/A	N/A	N/A	0x14 (0.020)	0x14 (0.020)
	MIFPGA0	N/A	N/A	N/A	0x23 (0.035)	0x23 (0.035)
	MIFPGA1	N/A	N/A	N/A	0x11 (0.017)	0x11(0.017)
Cisco Nexus 9348D-GX2A (N9K-C9348D-GX2A)	IOFPGA	N/A	N/A	N/A	0x16 (0.022)	0x16 (0.022)
	MIFPGA0	N/A	N/A	N/A	0x8 (0.008)	0x8 (0.008)
	MIFPGA1	N/A	N/A	N/A	0x5 (0.005)	0x5 (0.005)

Table 3. Available EPLD Images for the Cisco Nexus 9500 Platform Switches

Component	EPLD Device	Release 10.1(2)	Release 10.2(1)	Release 10.2(2)	Release 10.2(3)	Release 10.3(1)
Supervisor A (N9K-SUP-A)	IOFPGA	0x31 (0.049)	0x31 (0.049)	0x31 (0.049)	0x31 (0.049)	**0x32 (0.050)**
Supervisor A+ (N9K-SUP-A+)	IOFPGA	0x17 (0.023)	0x17 (0.023)	0x17 (0.023)	0x17 (0.023)	**0x18 (0.024)**
Supervisor B (N9K-SUP-B)	IOFPGA	0x30 (0.049)	0x30 (0.049)	0x30 (0.049)	0x30 (0.049)	0x30 (0.049)
Supervisor B+ (N9K-SUP-B+)	IOFPGA	0x17 (0.023)	0x17 (0.023)	0x17 (0.023)	0x17 (0.023)	**0x18 (0.024)**

© 2022 – 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Component	EPLD Device	Release 10.1(2)	Release 10.2(1)	Release 10.2(2)	Release 10.2(3)	Release 10.3(1)
System Controller (N9K-SC-A)	IOFPGA	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)	0x22 (0.034)
32-port 100-Gigabit QSFP28 line card (N9K-X9432C-S)	IOFPGA	0x14 (0.020)	0x14 (0.020)	0x14 (0.020)	0x14 (0.020)	0x14 (0.020)
	MIFPGA	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)
32-port 100-Gigabit QSFP28 line card (N9K-X9732C-EX) (for -E fabric modules)	IOFPGA	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)
	MIFPGA	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)
32-port 100-Gigabit QSFP28 line card (N9K-X9732C-EXM) (for -E fabric modules)	IOFPGA	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)
	MIFPGA	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)
36-port 100-Gigabit QSFP28 line card (N9K-X9732C-FX)	IOFPGA	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)
	MIFPGA	0x2 (0.002)	0x2 (0.002)	0x2 (0.002)	0x2 (0.002)	0x2 (0.002)
16-port 400-Gigabit QSFP-DD line card (N9K-X9716D-GX)	IOFPGA	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)
	MIFPGA	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)
36-port 100-Gigabit QSFP28 line card (N9K-X9736C-EX)	IOFPGA	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	0x13 (0.019)	**0x14 (0.020)**
	MIFPGA	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)
36-port 100-Gigabit QSFP28 line card (N9K-X9736C-FX)	IOFPGA	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	**0x11 (0.017)**
	MIFPGA	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)
48-port 1/10GBASE-T and 4-port 40-Gigabit QSFP+ line card (N9K-X9464TX)	IOFPGA	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)
	MIFPGA	0x8 (0.008)	0x8 (0.008)	0x8 (0.008)	0x8 (0.008)	0x8 (0.008)
48-port 1-/10-/25-Gigabit SFP28 and 4-port 40-/100-Gigabit QSFP28 line card (N9K-X97160YC-EX)	IOFPGA	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	**0x15 (0.021)**
	MIFPGA	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)	0x5 (0.005)
48-port 10-Gigabit SFP+ and 4-port 100-Gigabit QSFP28 line card (N9K-X9788TC-FX)	IOFPGA	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	0x4 (0.004)	**0x7 (0.007)**
	MIFPGA	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)
48-port 10-Gigabit SFP+ and 4-port 100-Gigabit QSFP28 line card (N9K-X9788TC2-FX)	IOFPGA	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)	0x6 (0.006)
	MIFPGA	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)
Fabric module for Cisco Nexus 9504	IOFPGA	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	0x15 (0.021)	**0x18 (0.024)**

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Component	EPLD Device	Release 10.1(2)	Release 10.2(1)	Release 10.2(2)	Release 10.2(3)	Release 10.3(1)
100-Gigabit -EX line (N9K-C9504-FM-E)						
Fabric module for Cisco Nexus 9504 100-Gigabit -S line cards (N9K-C9504-FM-S)	IOFPGA	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)
Fabric module for Cisco Nexus 9508 100-Gigabit -EX line cards (N9K-C9508-FM-E)	IOFPGA	0x14 (0.020)	0x14 (0.020)	0x14 (0.020)	0x14 (0.020)	0x14 (0.020)
Fabric module for Cisco Nexus 9508 100-Gigabit -EX line (N9K-C9508-FM-E2)	IOFPGA	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	**0x11 (0.017)**
Fabric module for Cisco Nexus 9508 100-Gigabit -S line (N9K-C9508-FM-S)	IOFPGA	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)	0x11 (0.017)
Fabric module for Cisco Nexus 9516 100-Gigabit -EX and -FX line cards (N9K-C9516-FM-E2)	MIFPGA	0x11 (0.011)	0x11 (0.011)	0x11 (0.011)	0x11 (0.011)	0x11 (0.011)
	IOFPGA	0x8 (0.008)	0x8 (0.008)	0x8 (0.008)	0x8 (0.008)	0x8 (0.008)

Table 4. Available EPLD Images for the Cisco Nexus 9500 Platform Switches with R Line Cards

Component	EPLD Device	Release 10.1(2)	Release 10.2(1)	Release 10.2(2)	Release 10.2(3)	Release 10.3(1)
36-port 100-Gigabit QSFP28 line card (N9K-X9636C-RX)	IOFPGA	0x18 (0.024)	0x18 (0.024)	0x18 (0.024)	0x18 (0.024)	0x18 (0.024)
	MIFPGA	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)
36-port 100-Gigabit QSFP28 line card (N9K-X9636C-R)	IOFPGA	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)	0x12 (0.018)
	MIFPGA	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)	0x9 (0.009)
36-port 40-Gigabit QSF+ line card (N9K-X9636Q-R)	IOFPGA	0x19 (0.025)	0x19 (0.025)	0x19 (0.025)	0x19 (0.025)	0x19 (0.025)
	MIFPGA	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)	0x3 (0.003)
52-port 100-Gigabit -R line cards (N9K-X96136YC-R)	IOFPGA	0xD	0xD	0xD	0xD	0xD
	MIFPGA	0xF	0xF	0xF	0xF	0xF
	DBFPGA	0xE	0xE	0xE	0xE	0xE

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Fabric module for Cisco Nexus 9504 100-Gigabit -R line cards (N9K-C9504-FM-R)	IOFPGA	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)	0x7 (0.007)
Fabric module for Cisco Nexus 9508 100-Gigabit -R line cards (N9K-C9508-FM-R)	IOFPGA	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)	0x10 (0.016)

Table 5. Available EPLD Images for the Cisco Nexus 9800 Platform Switches

Determining Whether to Upgrade EPLD Images

If the current EPLD image number for a card is greater than or matches the version expected for your current NXOS software version, you can skip the upgrade.

- To determine the EPLD upgrades needed for a Cisco Nexus 9000 Series switch running 10.3(1) software, use the **show install impact epld bootflash:<filename>** command on that switch, where the filename given for this release is the n9000-epld.10.3.1.img file. First, copy this file to the bootflash to proceed. In this example, the MIFPGA and IOFPGA EPLD images do not need to be upgraded.

Note: The CLI content in this document is only an example. The CLI output might change depending on the hardware/software.

switch# **show install all impact epld n9000-epld.10.3.1.img**

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to the table:

```
Module  Type   EPLD            Running-Version   New-Version  Upg-Required
------ ---- -------------    ---------------  ----------- ------------
   1    LC  MI FPGA              0x0f       0x0f          No
   1    LC  IO FPGA              0x0d       0x0d          No
   1    LC  DB FPGA              0x0e       0x0e          No
  21    FM  IO FPGA              0x07       0x07          No
  27   SUP  IO FPGA              0x15       0x15          No
  28   SUP  IO FPGA              0x15       0x15          No
  29    SC  IO FPGA              0x20       0x20          No
  30    SC  IO FPGA              0x20       0x20          No
```

Compatibility check:

```
Module       Type        Upgradable       Impact   Reason
```

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

```
----------------------------------------------
   1        LC        Yes      disruptive   Module Upgradable
  21        SUP       Yes      disruptive   Module Upgradable
  27        SUP       Yes      disruptive   Module Upgradable
  28        SUP       Yes      disruptive   Module Upgradable
  29        SC        Yes      disruptive   Module Upgradable
  30        SC        Yes      disruptive   Module Upgradable
```

Upgrade During ISSU

This feature offers the option to upgrade EPLD images during disruptive system (NXOS) upgrade. You will designate the target EPLD image using the ISSU command. The EPLD image will be validated during the pre-upgrade stage of the installation and the actual EPLD upgrade will be done before reloading the system. When the system comes back online, all EPLDs and the NXOS system images (including any required BIOS update) will be upgraded to the new versions.

To upgrade your EPLD image using the ISSU command, enter the NXOS and EPLD image to be installed using the **install all nxos <nxos-image> epld <epld-image>** command.

For additional information about ISSU, please see the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide.

Displaying the Status of EPLD Upgrades

To display the status of EPLD upgrades on the switch, use the **show install epld status** command.

Limitations

When EPLDs are upgraded, apply these guidelines and observations:

- If a module is not online, you cannot upgrade its EPLD images.
- If there are two supervisors that are installed in the switch (Cisco Nexus 9504, 9508, and 9516 switches only), you can either upgrade only the standby or upgrade all modules (including both supervisor modules) by using these commands:
    - **install epld bootflash:** image module standby-supervisor-slot-number (upgrades only the standby supervisor module)

Note: After you use this command, you can switchover the active and standby supervisor modules and then upgrade the other supervisor.

    - **install epld bootflash:** image module all (upgrades all of the modules)
- If there is only one supervisor that are installed in the switch, your upgrading or downgrading of EPLD images is disruptive.

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Secure Boot Hardware Tampering Vulnerability

This section details updating your EPLD version for affected switches listed in the link below. The table provides the PIDs exposed to the issue, as well as the fixed IO FPGA version for each PID, for validation purposes.

Secure Boot Hardware Tampering Vulnerability advisory:
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot

Vulnerable Products

These are the vulnerable products addressed in the Secure Boot Tampering Security Advisory (cisco-sa-20190513-secureboot).

Table 6. Nexus 9000 Series Switches affected by the Secure Boot Hardware Tampering Vulnerability

PID	Fixed IO FPGA Version
N9K-C93180YC-EX	0x15
N9K-C93108TC-EX	0x15
N9K-C93180YC-FX	0x20
N9K-C93108TC-FX	0x20
N9K-C9348GC-FXP	0x10
N9K-C93240YC-FX2	0x10
N9K-C9336C-FX2	0x10
N9K-C9364C	0x6
N9K-C9332C	0x10
N9K-C93180YC-FX	0x20
N9K-C9232C	0x8
N9K-SUP-A+	0x14
N9K-SUP-B+	0x14
N9K-SUP-B	0x30
N9K-SUP-A	0x30

© 2022 – 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Cisco Secure Boot Hardware Tampering Vulnerability - Remediation Steps

Nexus 9000 Modular chassis with dual supervisor

Note: Requirement–Update both Golden and Primary regions of FPGA to address this particular vulnerability. It is by design that we don't allow updating both primary and golden at the same time (to avoid programming errors that may cause switch to not boot, so only one region is allowed to be programmed per reload).

Please do not attempt to upgrade Golden region of the FPGA once it is on a fixed version.

1. Copy the EPLD image to bootflash (e.g., this document will use the n9000-epld.10.3.1.img image).
2. If you have dual supervisors, determine which is the standby supervisor by doing **'show module'** to verify the status of the supervisors, and start upgrading the standby first. On the Nexus 9500, only supervisors need to be upgraded to address this vulnerability. Line cards/fabric modules/system controllers are not affected.
3. Assuming the standby supervisor is slot 28, update the Primary FPGA region of the standby supervisor.

install epld bootflash:n9000-epld.10.3.1.img module 28

Expected result: The switch will update the primary EPLD of the standby supervisor and will reload the standby supervisor module automatically. Please don't interrupt, power cycle, or reload when EPLD update is happening. Once the standby is rebooted, it will again come up as the standby supervisor. The command **show version module 28 epld** will continue to show the old version.

Note: The CLI sequence used in this document is just an example. Your CLI sequence can be confirmed directly on the switch.

switch# show mod | grep SUP

```
27   0    Supervisor Module              N9K-SUP-A          active *
28   0    Supervisor Module              N9K-SUP-A          ha-standby        <<< standby supervisor
27   9.3(0.416)            1.0    SUP1
28   9.3(0.416)            0.3011 SUP2
```

switch# show version module 28 epld

```
EPLD Device                 Version
---------------------------------------
IO FPGA                     0x27
```

This is expected, as the switch would have booted from Golden FPGA which is still not updated. You can verify this from the syslog which would say:

%CARDCLIENT-5-MOD_BOOT_GOLDEN: Module 28 IOFPGA booted from Golden

4. Update the Golden (also called backup) FPGA region of the standby supervisor.

install epld bootflash:n9000-epld.10.3.1.img module 28 golden

Module 28 : IO FPGA [Programming] : 100.00% (64 of 64 total sectors)

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Module 28 EPLD upgrade is successful.

Module Type Upgrade-Result

------ ------------------ --------------

28 SUP Success

Expected result: Switch will update the golden EPLD of the standby supervisor and will reload the standby supervisor module automatically. Please don't interrupt, power cycle, or reload when EPLD update is happening. Once standby is booted, it will again come up as the standby supervisor.

Once this is done, check **show version module 28 epld** to confirm the FPGA version is greater than or equal to the fixed version for the standby supervisor. Your switch has the fixed version for standby supervisor.

switch# show version module 28 epld

EPLD Device Version

IO FPGA 0x30

Repeat Steps 3 and 4 for the active supervisor. At the end of Step 3, the supervisor in slot 27 will reload and so now will become the standby supervisor. The active supervisor will be the supervisor in slot 28.

For the situation where the active supervisor is in the other slot, considering SUP 27 is active to begin with, for the above activity, such as Steps 3 and 4, commands would have swapped 27 in place of 28.

Log below shows what happens when the EPLD upgrade happens for the active supervisor:

Module 27 : IO FPGA [Programming] : 100.00% (64 of 64 sectors)

Module 27 EPLD upgrade is successful.

Module Type Upgrade-Result

------ ------------------ --------------

27 SUP Success

EPLDs upgraded. Performing switchover.

Once the supervisor in Slot 27 becomes ha-standby, complete Step 4 for Slot 27 and it will again boot and become the ha-standby. Both the supervisors now have the vulnerability fixed version of the FPGA.

At the end of the upgrades, the switch should boot with the primary EPLD image for both SUPs, as seen in the logs below:

switch# show logging log | grep -i fpga | grep -i 27

2019 Jul 10 07:55:04 switch %CARDCLIENT-5-MOD_BOOT_PRIMARY: Module 27 IOFPGA booted from Primary

switch# show logging log | grep -i fpga | grep -i 28

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

2019 Jul 10 07:58:01 switch %CARDCLIENT-5-MOD_BOOT_PRIMARY: Module 28 IOFPGA booted from Primary

Nexus 9000 Modular chassis with single supervisor

Note: **Requirement–Update both Golden and Primary regions of FPGA to address this vulnerability.** It is by design that we don't allow updating both primary and golden at the same time (to avoid programming errors that may cause switch to not boot, so only one region is allowed to be programmed per reload).

Please do not attempt to upgrade Golden region of FPGA once it is on a fixed version.

1. Copy the EPLD image to bootflash (e.g., this document will use the n9000-epld.10.3.1.img image).
2. Assuming the supervisor is in slot 27, update the Primary FPGA region.

install epld bootflash:n9000-epld.10.3.1.img module 27

Expected result: Switch will update the primary EPLD of the supervisor and will reload the switch automatically. Please don't interrupt, power cycle, or reload when EPLD update is happening. Once the supervisor is booted, the command **show version module 27 epld** will continue to show the old version.

Note: The CLI sequence used in this document is just an example. Your CLI sequence can be confirmed directly on the switch.

Switch#show version module 27 epld

```
------------------------------------------------------------------
Name                InstanceNum         Version       Date
------------------------------------------------------------------
IO FPGA                    0              0x27       20160111
BIOS version                v08.35(08/31/2018)
Alternate BIOS version      v08.32(10/18/2016)
```

This is expected, as the switch would have booted from the Golden FPGA which is still not updated. You can verify this from the syslog which would say:

%CARDCLIENT-5-MOD_BOOT_GOLDEN: Module 27 IOFPGA booted from Golden

3. Since in this case there is only one supervisor, next update the Golden (also called the backup) FPGA region.

install epld bootflash:n9000-epld.10.3.1.img module 27 golden

Module 27 : IO FPGA [Programming] : 100.00% (64 of 64 total sectors)

Module 27 EPLD upgrade is successful.

```
Module       Type  Upgrade-Result
------ ------------------ --------------
  27        SUP        Success
```

Expected result: The switch will update the golden EPLD of the supervisor and will reload the switch automatically. Please don't interrupt, power cycle, or reload the device while the EPLD update is in progress.

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Once this is done, when you check the command **show version module 27 epld** to confirm that the FPGA version is greater than or equal to the fixed version for the supervisor. Your supervisor now has the vulnerability fixed version of FPGA.

Switch# show version module 27 epld

```
------------------------------------------------------------------
Name                InstanceNum         Version       Date
------------------------------------------------------------------
IO FPGA                    0              0x30       20190625
BIOS version                v08.35(08/31/2018)
Alternate BIOS version      v08.32(10/18/2016)
```

At the end of the upgrades, the switch should boot with the primary EPLD for the supervisor. The log to check is seen below:

switch# show logging log | grep -i fpga | grep -i 27

2019 Jul 10 07:55:04 switch %CARDCLIENT-5-MOD_BOOT_PRIMARY: Module 27 IOFPGA booted from Primary

IMPORTANT NOTE:

If you attempt to upgrade the Golden region of the FPGA once it is on the fixed version, the system will not automatically allow you to upgrade the Golden region of the supervisor and will provide the prompt seen below:

switch# install epld bootflash:n9000-epld.10.3.1.img module all golden

Digital signature verification is successful

Compatibility check:

Module	Type	Upgradable	Impact	Reason
22	FM	Yes	disruptive	Module Upgradable
24	FM	Yes	disruptive	Module Upgradable
27	SUP	No	none	Golden Not Upgradable
28	SUP	No	none	Golden Not Upgradable
29	SC	Yes	disruptive	Module Upgradable
30	SC	Yes	disruptive	Module Upgradable

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Retrieving EPLD versions.... Please wait.

Images will be upgraded according to this table:

Module	Type	EPLD	Running-Version	New-Version	Upg-Required
22	FM	IO FPGA	0x19	0x19	Yes
24	FM	IO FPGA	0x19	0x19	Yes
29	SC	IO FPGA	0x17	0x20	Yes
30	SC	IO FPGA	0x17	0x20	Yes

Module 27 (EPLD ver 0x29) Golden upgrade not supported

Module 28 (EPLD ver 0x30) Golden upgrade not supported

The above modules require upgrade.

Since both System Controller modules need an upgrade,a chassis reload will happen at the end of the upgrade.

Do you want to continue (y/n) ? [n] y

Nexus 9000 TOR (standalone chassis) switch

Note: It is required to update both the Golden and Primary regions of the FPGA to address this vulnerability. It is by design that we don't allow updating both primary and golden at the same time (to avoid programming errors that may lead to switch boot failure), so only one FPGA region is allowed to be programmed per reload.

Please do not attempt to upgrade Golden region of FPGA once it is on a fixed version.

1. Copy the EPLD image to bootflash (e.g., this document will use the n9000-epld.10.3.1.img image).
2. Update the Primary FPGA region.

install epld bootflash:n9000-epld.10.3.3.img module all

Expected result: The switch will update the EPLD and will reload automatically. Please don't interrupt, power cycle, or reload the switch while the EPLD update is in progress. The switch will boot up with the golden FPGA. The command **show version module 1 epld** will show the old IO FPGA version at this time. This is expected.

Note: The CLI sequence used in this document is just an example. Your CLI sequence can be confirmed directly on the switch.

Switch# show version module 1 epld

Name	InstanceNum	Version	Date
IO FPGA	0	0x06	20180920
MI FPGA	0	0x01	20170609

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

BIOS version v01.14(06/15/2019)

Alternate BIOS version v01.12(07/25/2018)

You can verify this from syslog which would say:

%CARDCLIENT-5-MOD_BOOT_GOLDEN: Module 1 IOFPGA booted from Golden

%CARDCLIENT-2-FPGA_BOOT_GOLDEN: IOFPGA booted from Golden

3. Update the Golden (also called backup) FPGA region.

install epld bootflash:n9000-epld.10.3.1.img module all golden

Expected result: The switch will update the EPLD image and will reload automatically. Please don't interrupt, power cycle, or further reload the switch when the EPLD update is in progress.

Once this is done, when you check **show version module 1 epld**, you will see an FPGA version that is greater than or equal to the fixed version.

Switch# show version module 1 epld

Name InstanceNum Version Date

IO FPGA 0 0x07 20180920

MI FPGA 0 0x01 20170609

BIOS version v01.14(06/15/2019)

Alternate BIOS version v01.12(07/25/2018)

After the upgrade is complete, the switch should boot up with the primary EPLD image as shown in the logs below:

Switch# show logging log | grep -i fpga

2019 Jul 9 19:46:11 switch %CARDCLIENT-2-FPGA_BOOT_PRIMARY: IOFPGA booted from Primary

2019 Jul 9 19:46:11 switch %CARDCLIENT-2-FPGA_BOOT_PRIMARY: MIFPGA booted from Primary

2019 Jul 9 19:46:11 switch %CARDCLIENT-5-MOD_BOOT_PRIMARY: Module 1 IOFPGA booted from Primary

2019 Jul 9 19:46:11 switch %CARDCLIENT-5-MOD_BOOT_PRIMARY: Module 1 MIFPGA booted from Primary

Related Documentation

The entire Cisco NX-OS 9000 Series documentation set.

Release Notes

The entire Cisco NX-OS 9000 Series release notes set.

© 2022 - 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus9k-docfeedback@cisco.com. We appreciate your feedback.

Legal Information

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: https://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. (1110R)

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.

© 2024 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://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: https://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. (1110R)

© 2022 – 2024 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential