FPGA/EPLD Upgrade Precedure to Address Secure Boot Vulnerability

This document describes how to update the EPLD using the Generic EPLD update image for use with the Cisco Nexus 9000 Series switches and Cisco Nexus 3000 Series switches running 7.0(3)I4(x), 7.0(3)I7(1) to 7.0(3)I7(6) and 9.2(1) to 9.2(3) to address the Secure Boot Vulnerability detailed here. This EPLD update is a complimentary update to whatever EPLD software that shipped with the respective software, and hence can be additively applied to these versions. The update images are listed below and should be available against the 'NX-OS EPLD Updates' section of the latest maintenance release for each of the above trains.

- For Cisco Nexus 9000 and 3000 Series switches - n9000-epld-secure-boot-update.img

For the affected switches mentioned in Table 1. Vulnerable Products addressed in Security Advisory (cisco-sa-20190513-secureboot)

Note: 9.3(1), 9.2(4) and 7.0(3)I7(7), will have this complimentary update built into their EPLD release update, and hence no need to apply this complimentary EPLD update. Please follow this link for N9K-C93180LC-EX

Table of Contents

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.

Deciding 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.

> NOTE: Do not perform an EPLD upgrade during an ISSU system upgrade.

Switch Requirements

The Cisco Nexus 9000 Series switch must be running the Cisco NX-OS operating system and include the following hardware:

- Supervisor modules (2)–each with at least 800 MB of available boot flash memory (Cisco Nexus 9504, 9508, and 9516 switches)
- System controller modules (2) (Cisco Nexus 9504, 9508, and 9516 switches)
- Line cards (Cisco Nexus 9504, 9508, and 9516 switches)
  - Cisco Nexus 9504 switch (1 to 4 line cards)
  - Cisco Nexus 9508 switch (1 to 8 line cards)
  - Cisco Nexus 9516 switch (1 to 16 line cards)
- Fabric modules (Cisco Nexus 9504, 9508, and 9516 switches)
  - Fabric modules for 40-Gigabit line cards on a Cisco Nexus 9504, 9508, or 9516 switch (3-6 modules)

  - Fabric modules for 100-Gigabit –E line cards on a Cisco Nexus 9504, 9508, or 9516 switch (4 modules)
  - Fabric modules for 100-Gigabit –S line cards on a Cisco Nexus 9504 or 9508 switch (4 modules)
- Fan modules
  - Cisco Nexus 92304QC, 9272Q, and 93120TX switches (2 modules)
  - Cisco Nexus 9336C-FX2, 9364C, 9396PX, 9396TX, and 93128TX switches (3 modules)
  - Cisco Nexus 9236C, 92160YC-X, 92300YC, 9332PQ, 9372PX, 9372PX-E, 9372TX, 9372TX-E, 93108TC-EX, and 93180LC-EX switches (4 modules)
  - Cisco Nexus 9332C, and 93240YC-FX2 switch (5 modules)
  - Cisco Nexus 9504, 9508, and 9516 switches (3 fan trays)
- Power supplies
  - 500-W AC, 930-W DC, or 1200-W HVAC/HVDC power supplies (2 for the Cisco Nexus 93180LC-EX switches)
  - 650-W AC, 930-W DC, or 1200-W HVAC/HVDC power supplies (2 for the Cisco Nexus 92160YC-X, 92304QC, 9236C, 93108TC-EX, 93180YC-EX, 9332PQ, 9372PX, 9372PX-E, 9372TX, 9372TX-E, 9396PX, and 9396TX switches
  - 650-W AC or 1200-W HVAC/HVDC power supplies (2 for Cisco Nexus 92300YC switches)
  - 930-W DC power supplies (2 for all Cisco Nexus 9200 and 9300 platform switches (except 92300YC and 9348GC-FXP switches)
  - 11000W AC power supplies (2) for the Cisco Nexus 9332C, 9336C and 93240YC switches
  - 11000W DC power supplies (2) for the Cisco Nexus 9332C, 9336C and 93240YC switches
  - 11000W HVAC/HVDC power supplies (2) for the Cisco Nexus 9336C and 93240YC switches
  - 1200-W AC power supplies (2) or 930-W DC power supplies (2) for the Cisco Nexus 9272Q, 93120TX, 93128TX, and 9364C switches
  - 1200-W HVAC/HVDC power supplies (2) for all Cisco Nexus 9200 and 9300 platform switches (except the 9348GC-FXP switch)
  - 3000-W AC power supplies or 3000-W Universal AC/DC or 3000-W DC power supplies for Cisco Nexus 9500 switches
  - 3.15-kW dual input universal AC/DC power for the Cisco Nexus 9500 switches
    - Cisco Nexus 9504 switch (up to 4)
    - Cisco Nexus 9508 switch (up to 8)
    - Cisco Nexus 9516 switch (up to 10)
- Uplink module (Cisco Nexus 93128TX, 9396PX, and 9396TX switches only)
  - M4PC-CFP2
  - M6PQ

- M6PQ-E
- M12PQ

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 7.0(3)I4(x) through 9.2(x)

Each EPLD image that you can download from https://software.cisco.com/download/navigator.html is a bundle of EPLD upgrades. To see the recent updated EPLD versions for the Cisco Nexus 9200, 9300, 9300-EX, 9300-FX, and 9500 platforms, see the following 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: The n9000-epld.secure-boot.img EPLD, addresses the Secure Boot Hardware Tampering vulnerability for the Nexus 3K and Nexus 9000 Series switches. Please refer to Security Advisory at https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot.

Please review the advisory for affected HW-PIDs (see below table) for more details on how to apply the patch. The n9000-epld.secure-boot.img epld requires a specific sequence of upgrade.

Table 1. Vulnerable Products addressed in Security Advisory (cisco-sa-20190513-secureboot)

Nexus 9000 Series Switches

PID	Fixed IO FPGA Version
N9K-C93180YC-EX	0x15
N9K-C93108TC-EX	0x15
N9K-C93180LC-EX	0x20
N9K-C93180YC-FX	0x20
N9K-C93108TC-FX	0x20
N9K-C9348GC-FXP	0x10
N9K-C92300YC	0x20
N9K-C93240YC-FX2	0x10
N9K-C9336C-FX2	0x10
N9K-C9364C	0x6
N9K-C9332C	0x10
N9K-C92160YC-X	0x19
N9K-C9272Q	0x17
N9K-C92304QC	0x12

N9K-C9236C	0x17
N9K-C9232C	0x8
N9K-SUP-A+	0x14
N9K-SUP-B+	0x14
N9K-C93120TX	0x13
N9K-SUP-B	0x30
N9K-SUP-A	0x30

Nexus 3000 Series Switches

N3K-C36180YC-R	0x8
N3K-C3636C-R	0x8
N3K-3232C	0x12
N3K-C3264Q-S	0x12
N3K-C31108PC-V	0x6
N3K-C3164Q-40GE	0x13
N3K-C31108TC-V	0x6
N3K-C3132C-Z	0x20
N3K-C3264C-E	0x6

NOTE: N3K-C36180YC-R and N3K-C3636C-R, CPU FPGA will have the fix, so look for CPU FPGA instead of IO.

Cisco Secure Boot Hardware Tampering Vulnerability - Remediation Steps

The following section details updating your EPLD version for affected switches listed in:
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot

Nexus 9000 Modular chassis with dual supervisor:

IMPORTANT NOTE:
It is required to 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, hence 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. used n9000-epld.secure-boot.img).
2. If you have dual supervisor, determine which is the standby Supervisor by doing 'show module' and start upgrading it first. On the N9K, Only supervisors need upgrade for this vulnerability. LC/FM/SC cards are not affected.
3. Assuming standby supervisor is slot 28. Update the Primary FPGA region of standby supervisor.

```
install epld bootflash:n9000-epld.secure-boot.img module 28
```

Expected result: Switch will update primary EPLD of 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 standby supervisor. A 'show version module 28 epld' will continue to show old version.

```
switch# show mod | grep SUP
27   0    Supervisor Module              N9K-SUP-A          active *
28   0    Supervisor Module              N9K-SUP-A          ha-standby
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 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.secure-boot.img module 28 golden[1]

```
Module 28 : IO FPGA [Programming      ] : 100.00% (     64 of      64 total sectors)
Module 28 EPLD upgrade is successful.
Module       Type  Upgrade-Result
------  ------------------  --------------
   28        SUP        Success
```

Expected result: Switch will update the golden EPLD of 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 ha-standby supervisor.
Once this is done, when you check 'show version module 28 epld' you will see FPGA version that is >= 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 Step 3 and 4, for the active supervisor. At the end of Step 3, supervisor in slot 27 will reload and hence now will become standby supervisor. The active supervisor will be Supervisor in slot 28.

(considering SUP 27 is active to begin with, for the above activity, such as steps 3 and 4, commands would have 27 in place of 28.)

Log below shows what happens when epld upgrade happens for active supervisor.

[1] The golden keyword used here for upgrade, is not available for command completion.

```
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 ha-standby. Both the supervisors now have the vulnerability fixed version of FPGA.

At the end of the upgrades, switch should boot with primary for both SUPs, 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
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:

IMPORTANT NOTE:
It is required to 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, hence 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. used n9000-epld.secure-boot.img).

2. Assuming the supervisor is in Slot27. Update the Primary FPGA region.

install epld bootflash:n9000-epld.secure-boot.img module 27

Expected result: Primary EPLD of the supervisor will get upgraded and will cause a switch reload. Please don't interrupt, power cycle or reload when EPLD update is happening. Once the supervisor is booted, the 'show version module 27 epld' will continue to show old version

```
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 Golden FPGA which is still not updated. You can verify this from sys-log which would say:

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

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

```
install epld bootflash:n9000-epld.secure-boot.img module 27 golden[2]

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 golden EPLD of the supervisor will get upgraded and will cause a switch reload. Please don't interrupt, power cycle or reload when EPLD update is happening.
Once this is done, when you check 'show version module 27 epld' you will see FPGA version that is >= to the fixed version for the supervisor. Your supervisor 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, switch should boot with primary for the SUP, log 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
```

Nexus 9000 and Nexus 3000 TOR:

IMPORTANT NOTE:
It is required to 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, hence 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. used n9000-epld.secure-boot.img).
2. Update the Primary FPGA region.

```
install epld bootflash:n9000-epld.secure-boot.img module 1
```

Expected result: Switch will update EPLD and will reload automatically. Please don't interrupt, power cycle or reload when EPLD update is happening. Switch would boot up with golden FPGA, 'show version module 1 epld' would show the old Fpga version for IO, due to this. This is expected.

```
show version module 1 epld
-----------------------------------------------------------------
```

[2] The goldedn keyword used here for upgrade, is not available for command completion.

```
Name                  InstanceNum        Version      Date
-----------------------------------------------------------------
IO FPGA                  0            0x06      20180920
MI FPGA                  0            0x01      20170609
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.secure-boot.img module 1 golden[3]

Expected result: Switch will update EPLD and will reload automatically. Please don't interrupt, power cycle or reload when EPLD update is happening.

Once this is done, when you check 'show version module 1 epld' you will see FPGA version that is >= to the fixed version.

```
show version module 1 epld
-----------------------------------------------------------------
Name                  InstanceNum        Version      Date
-----------------------------------------------------------------
IO FPGA                  0            0x07      20190607
MI FPGA                  0            0x01      20170609
BIOS version                v01.14(06/15/2019)
Alternate BIOS version         v01.12(07/25/2018)
```

After upgrade is complete, switch should boot up with primary, shown logs below

```
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
```

NOTE: For N3K-C36180YC-R and N3K-C3636C-R, CPU FPGA will have the fix, so look for CPU FPGA instead of IO.

[3] The goldedn keyword used here for upgrade, is not available for command completion.

Downloading the EPLD Images

Before you can prepare the EPLD images for installation, you must download them to the FTP or management server.

1. From a browser, go to https://software.cisco.com/download/navigator.html.

   The browser displays the Cisco website.

2. Choose Switches.

   A list of switch types displays on the right.

3. Select Data Center Switches.

   The right side lists the Data Center Switch product series.

4. Select Cisco Nexus 9000 Series Switches or Nexus 3000 Series Switches.

   The right side lists the switches in the series that you selected.

5. Select the switch that you are updating EPLD images for.

   The Downloads page opens and lists what you can download for the switch that you selected.

6. Select NX-OS EPLD Updates.

   The Download Software page lists the available EPLD images for the switch.

7. If you see a new EPLD image for the NX-OS software installed on the switch, click the Download button.

   CAUTION: When you are trying to upgrade EPLD, it is recommended to use the same version of EPLD as that of installed software. However, if the installed version of EPLD is already later than the software you are installing, NX-OS software does not allow for the downgrading of the EPLD. Newer EPLD is compatible with older NX-OS software.

8. Click the link for the file.

   The Downloads page displays a Download button and lists information for the file.

9. Click Download.

   The Supporting Documents page opens to display the rules for downloading the software.

10. Read the rules and click Agree.

    A File Download dialog box opens to ask if you want to open or save the images file.

11. Click Save.

    The Save As dialog box appears.

12. Indicate where to save the file and click Save.

    The file saves to the location that you specified.

Installation Guidelines

To upgrade the EPLD images using CLI commands, follow these guidelines:

- Before you upgrade any EPLD images, be sure that you have updated the Cisco NX-OS operating system to the level required for the images. Also be sure that you have an EPLD image file.

CAUTION: When you are trying to upgrade EPLD, it is recommended to use the same version of EPLD as that of installed software. However, if the installed version of EPLD is already later than the software you are installing, it is not required to downgrade the EPLD.

- You can execute an upgrade from the active supervisor module only. This upgrade is for one or all of the modules as follows:
  - You can upgrade a module individually.
  - You can upgrade all modules sequentially.
  - You can update the images for online modules only.
- On a Cisco Nexus 9500 platform switch that has two supervisor modules, upgrade the EPLDs for the standby supervisor and then switch the active supervisor to the standby mode to upgrade its EPLDs. The supervisor switchover is not disruptive to traffic on Cisco Nexus 9500 platform switches. On a switch that has only one supervisor module, you can upgrade the active supervisor, but this will disrupt its operations during the upgrade.
- If you interrupt an upgrade, you must reapply the upgrade to the module that was being upgraded during the interruption.
- The upgrade process disrupts traffic on the targeted module.
- Do not insert or remove any modules while an EPLD upgrade is in progress.

1. Copy the EPLD image file to bootflash.
2. To determine if you need to upgrade the BIOS for the image, use the show install all impact command and see the Upgrade Required (Upg-Required) field for the BIOS row in the command output.
3. Enter the install epld bootflash:n9000-epld.secure-boot.img module all command.

   The switch automatically reboots.

Upgrading the EPLD Images

CAUTION: When you are trying to upgrade EPLD, it is recommended to use the same version of EPLD as that of installed software. However, if the installed version of EPLD is already later than the software you are installing, it is not required to downgrade the EPLD.

Verifying the EPLD Upgrades

To verify the EPLD upgrades for a switch or its modules, use the show version module *slot-number* epld command as follows:

- To verify updates for a module on a modular switch (Cisco Nexus 9500 platform switches), indicate the chassis slot number for *slot-number.*
  `switch# show version module 27 epld`
- To verify updates for a top-of-rack switch (Cisco Nexus 9200, 9300, and 9300-EX platforms), use 1 for *slot-number*.
  `switch# show version module 1 epld`

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, the following guidelines and observations apply:

- 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 the following 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.

Related Documentation

The entire Cisco NX-OS 9000 Series documentation set is available at the following URL:
https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

Release Notes

The release notes are available at the following URL:
https://www.cisco.com/en/US/products/ps13386/prod_release_notes_list.html

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.

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*, at:
https://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*. It lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.