Instructions for Addressing the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco ASR 1000 Series Routers

Information about Upgrading ASR 1000 Modular Chassis 2

Information about Upgrading Cisco ASR 1000 Consolidated Chassis 14

Revised: September 15, 2022

Information about Upgrading ASR 1000 Modular Chassis

Upgrading the router to fix this hardware vulnerability involves two steps:

- **Running an IOS XE tool to fix the vulnerability** - As part of this step, download the tool from the Cisco software downloads page. The name of this tool is `asr1000rpx86-universalk9.V1612_1_CVE_2019_1649.SPA.bin`.This tool installs an IOS XE image on the active and standby RP cards. During installation of this tool, all the RPs, ESP's and carrier cards are automatically detected and the CPLD version is checked. If the CPLD version is found to be vulnerable to the security vulnerability, the CPLD is automatically upgraded. This IOS XE tool covers the upgrade needs of all the three field replaceable units – Route Processor, Embedded Service Processors and Ethernet Line Cards.

- **Booting the router** - To confirm that upgrading was successful and that the vulnerability was fixed, boot the router with the existing IOS XE image and verify the version of CPLD with details given in Table 1.

Note The platforms that are affected by this hardware vulnerability are listed in Table 1. It is strongly recommended to not run the IOS XE tool on any other platforms. If you are on an ASR 1000 modular chassis and have installed an ASR1000-RP2 module, then the IOS XE tool upgrades the CPLD for rest of the line cards, but skips updating the CPLD for the ASR1000-RP2 module.

Prerequisites for Upgrading FPGA for ASR 1000 Modular Chassis

- If you are upgrading ASR1000-RP2, download `asr1000rpx86-universalk9.V1612_1_CVE_2019_1649.SPA.bin` from https://software.cisco.com/download/home/282450665/type/283425232/release/16.0.0 and copy it to the USB or bootflash of the router that is scheduled for upgrade.

  If you are upgrading ASR1000-RP3, download `asr1000rpx86-universalk9.V1612_1_CVE_2019_1649.SPA.bin` from https://software.cisco.com/download/home/286308009/type/283425232/release/16.0.0 and copy it to the USB or bootflash of the router that is scheduled for upgrade.

- The upgrade procedure is required only if the CPLD version of the FRU is below the recommended version. Before you attempt to upgrade the router, see *Checking the CPLD version section* for the recommended CPLD version.

- Run the **show platform** command and verify the output to ensure that all the FRU's are in `ok`, `ok,active` or `ok,standby` state.

- It is extremely important to ensure there is power redundancy to run the IOS XE tool on all the cards in the chassis. You can check this by using the **show platform** command.

Figure 1: Example of a show platform command with all modules and FRU's working correctly

```
Router#show platform
Chassis type: ASR1009-X

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1000-MIP100      ok                    00:24:56
 0/0      EPA-QSFP-1X100GE    ok                    00:21:49
1         ASR1000-6TGE        ok                    00:24:56
 1/0      BUILT-IN-6TGE       ok                    00:22:51
2         ASR1000-2T+20X1GE   ok                    00:24:56
 2/0      BUILT-IN-2T+20X1GE  ok                    00:22:56
R0        ASR1000-RP3         ok, active            00:24:56
R1        ASR1000-RP3         ok, standby           00:24:56
F0        ASR1000-ESP100      ok, active            00:24:56
F1        ASR1000-ESP100      ok, standby           00:24:56
P0        ASR1000X-AC-1100W   ok                    00:23:41
P1        ASR1000X-AC-1100W   ok                    00:23:38
P2        Unknown             empty                 never
P3        Unknown             empty                 never
P4        Unknown             empty                 never
P5        Unknown             empty                 never
P6        ASR1000X-FAN        ok                    00:23:26
P7        ASR1000X-FAN        ok                    00:23:23
P8        ASR1000X-FAN        ok                    00:23:24

Slot      CPLD Version        Firmware Version
--------- ------------------- ------------------------------------
0         15072100            16.3(2r)
1         13091900            16.3(2r)
2         14011701            16.3(2r)
R0        17042115            16.9(5r)
R1        17042115            16.9(5r)
F0        12071700            16.3(2r)
F1        12071700            16.3(2r)
```

520152

- Ensure that all the FRU's are on the latest recommended ROMmon software before triggering the upgrade using the IOS XE tool
- On a chassis with ASR1000-RP2 the recommended ROMmon version is 16.9(5r). In addition to this, also ensure that the FPGA version is greater than or equal to 17071402. This is required for loading the latest IOS images on the router
- If you are on ASR1000-RP3, run the **show diag slot R0 eeprom** command and in the output look for **`Top Assy. Part Number`**. If the last part of this value is less than or equal to 05, then a manual power-cycle is required at step 7 of the upgrade procedure.

```
Router#show diag slot R0 eeprom
Slot R0 EEPROM data:

        Product Identifier (PID) : ASR1000-RP3
        Version Identifier (VID) : V03
        PCB Serial Number        : JAE23110JQJ
        Top Assy. Part Number    : 68-5621-07
        Hardware Revision        : 1.0
        CLEI Code                : COUCAVLCAB
Router#
Router#sh diag slot R1 eeprom
Slot R1 EEPROM data:

        Product Identifier (PID) : ASR1000-RP3
        Version Identifier (VID) : V01
        PCB Serial Number        : JAE204603RL
        Top Assy. Part Number    : 68-5621-05
        Hardware Revision        : 1.0
        CLEI Code                : COUCAVBCAA
```

Upgrading FPGA for ASR 1000 Modular Chassis

Note If you attempt to boot a chassis that has an FRU with an FPGA version that is lower than expected you will see the following error:

```
CET:>
%CMFP-3-FPGA_IMG_ABSENT: F1: cman_fp: FPGA image is absent please contact Cisco technical
          support representative
```

To resolve this issue, upgrade the FPGA as per details in the following procedure:

To upgrade FPGA, run the upgrade utility image:

Procedure

Step 1 Confirm that both the RP 0 and RP 1 are in ISSU ready state. This state can be confirmed by using the **show redundancy** command.

```
show redundancy
Redundant System Information :
------------------------------
       Available system uptime = 3 minutes
Switchovers system experienced = 0
              Standby failures = 0
        Last switchover reason = none

                 Hardware Mode = Duplex
    Configured Redundancy Mode = sso
     Operating Redundancy Mode = sso
              Maintenance Mode = Disabled
                Communications = Up

Current Processor Information :
-------------------------------
               Active Location = slot 7
        Current Software state = ACTIVE
       Uptime in current state = 3 minutes
                 Image Version = Cisco IOS Software [Gibraltar], ASR1000 Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M)
, Version 16.12.1, RELEASE SOFTWARE (fc4)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compiled Tue 30-Jul-19 19:27 by mcpre

                          BOOT = harddisk:asr1000rpx86-universalk9.16.12.01.SPA.bin,12;

                   CONFIG_FILE =

        Configuration register = 0x2102


Peer Processor Information :
----------------------------
              Standby Location = slot 6
```

```
        Current Software state = STANDBY HOT
       Uptime in current state = 0 minutes
                 Image Version = Cisco IOS Software [Gibraltar], ASR1000 Software
(X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.1, RELEASE SOFTWARE (fc4)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compiled Tue 30-Jul-19 19:27 by mcpre

                          BOOT = harddisk:asr1000rpx86-universalk9.16.12.01.SPA.bin,12;

                   CONFIG_FILE =

        Configuration register = 0x2102
```

Step 2 Save the current running configuration and backup it to bootflash.

```
Router#copy running-config bootflash:running-config_17Dec2019
Destination filename [running-config_23Oct2019]?
6222 bytes copied in 0.536 secs (11608 bytes/sec)
Router#

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

Step 3 Note down the configuration register value and change it to `0x0`. At the last step of this procedure the configuration register is reset with the old value.

```
Router#show version | in configuration
Configuration register is 0x2102
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#config-register 0x0
Router(config)#end
Router#write
```

Step 4 Copy the IOS XE utility to USB or to bootflash: using FTP or TFTP command to both RP slot 0 and RP slot 1:

RP Slot 0

```
Router# copy  asr1000rpx86-universalk9.V1612_1_CVE_2019_1649.SPA.bin harddisk:
Destination filename [image name]?
Accessing  asr1000rpx86-universalk9.V1612_1_CVE_2019_1649.SPA.bin...
Loading  asr1000rpx86-universalk9.V1612_1_CVE_2019_1649.SPA.bin (via GigabitEthernet0): !!!!
[OK - 1078042481 bytes]

1078042481 bytes copied in 85.835 secs (12559474 bytes/sec)
Router#
```

RP Slot 1

```
Router#copy harddisk: asr1000rpx86-universalk9.V1612_1_CVE_2019_1649.SPA.bin stby-harddisk:

Destination filename [image name]?

Copy in progress...CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

```
1078042481 bytes copied in 195.013 secs (5528054 bytes/sec)
Router#
```

Step 5 Issue the **router reload** command on RP slot 0 and 1and ensure that the ROMmon prompt is displayed on the router

RP Slot 0

```
Router#reload
Proceed with reload? [confirm]
Initializing Hardware ...
System integrity status: 9B710000  12030000  A0A00A05
System Bootstrap, Version 16.9(5r), RELEASE SOFTWARE
Copyright (c) 1994-2019  by cisco Systems, Inc.
Current image running: Boot ROM0
Last reset cause: LocalSoft
ASR1000-RP3 platform with 8388608 Kbytes of main memory
rommon 1 >
```

RP Slot 1

```
Router-stby# reload
Initializing Hardware ...
System integrity status: 9B710000  12030000  A0A00A05
System Bootstrap, Version 16.9(5r), RELEASE SOFTWARE
Copyright (c) 1994-2019  by cisco Systems, Inc.
Current image running: Boot ROM1
Last reset cause: LocalSoft
ASR1000-RP3 platform with 8388608 Kbytes of main memory
rommon 1 >
```

Step 6 **Attention** The upgrade utility performs the upgrade task through several automated steps.

No manual intervention is required at any stage.

The upgrade process starts off by upgrading the RP and this takes about 20 minutes.

When this step is complete, the IOS copyright banner is displayed

After this the utility proceeds to upgrade each of the remaining line cards (except the other RP in a dual RP system)

After upgrade of each line card is completed, the router reboots and comes back online with an OK status.

After this the route processor power cycles the box and returns to ROMmon prompt.

You can now repeat the same procedure with the other RP.

The approximate time required to complete this process is about 30 minutes.

Note If you are on a system with dual ASR1000-RP2, you must run the IOS XE tool only on the active RP2 and not on the standby RP2 card.

RP 0

```
Rommon> boot harddisk:asr1000rpx86-universalk9.V1612_1_CSCVN77167.SPA.bin
File size is 0x4041ad8f
Located asr1000rpx86-universalk9.V1612_1_CSCVN77167.SPA.bin
Image size 1078046095 inode num 270338, bks cnt 263195 blk size 8*512
################################################################################################################################################

Boot image size = 1078046095 (0x4041ad8f) 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 16acc89c:916a2757:a9ac28c1:e5b88393:2ca73bab
        expected   16acc89c:916a2757:a9ac28c1:e5b88393:2ca73bab
Validating main package signatures

RSA Signed RELEASE Image Signature Verification Successful.
Image validated

This is the ACTIVE RP
Standby RP present - Hold it in reset

**************************************************
***         PSIRT FPGA UPGRADE REQUESTED         ***
***                                              ***
***        CURRENT CPLD VERSION: 17042115        ***
***                                              ***
***                UPGRADING FPGA                ***
***                                              ***
**************************************************
***                                              ***
***      WARNING !!  WARNING !! WARNING !!       ***
***                                              ***
*** DO NOT POWER CYCLE OR TURN OFF THE ROUTER !!! ***
***                                              ***
*** DO NOT ADD OR REMOVE CARDS FROM THE SYSTEM !! ***
***                                              ***
***  THIS MAY TAKE UP TO 20 MINUTES TO COMPLETE  ***
***                                              ***
**************************************************

****************************************
***  Upgrade completed on this card     ***
****************************************

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software [Gibraltar], ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.1,
 CUST-SPECIAL:V1612_1_CSCVN77167

This software is supported for a limited time under special agreement with Cisco Systems, Inc.
CSCvn77167
Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compiled Wed 11-Dec-19 02:06 by mcpre
```

```
This software version supports only Smart Licensing as the software licensing mechanism.


PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE,
AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE
"SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL
ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU
ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement
(EULA) and any relevant supplemental terms (SEULA) found at
http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

You hereby acknowledge and agree that certain Software and/or features are
licensed for a particular term, that the license to such Software and/or
features is valid only for the applicable term and that such Software and/or
features may be shut down or otherwise terminated by Cisco after expiration
of the applicable license term (e.g., 90-day trial period). Cisco reserves
the right to terminate any such Software feature electronically or by any
other means available. While Cisco may provide alerts, it is your sole
responsibility to monitor your usage of any such term Software feature to
ensure that your systems and networks are prepared for a shutdown of the
Software feature.



All TCP AO KDF Tests Pass
============================================================
==                  ACTIVE RP                               ==
==  WAITING FOR ALL LINECARDS TO BOOT AFTER FPGA UPGRADE ==
==                                                          ==
==    DO NOT POWER CYCLE OR TURN OFF THE ROUTER !!!      ==
============================================================
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting

============================================================
Waiting for linecards to remain stable
...................Waiting for card ASR1000-MIP100       in slot 0 - booting
.
============================================================
Waiting for card ASR1000-MIP100       in slot 0 - booting

Waiting for card ASR1000-MIP100       in slot 0 - booting
============================================================
Waiting for linecards to remain stable
............................................................
============================================================
============================================================
```

```
Chassis type: ASR1009-X

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1000-MIP100      ok                    00:25:14
1         ASR1000-6TGE        ok                    00:25:14
2         ASR1000-2T+20X1GE   ok                    00:25:14
R0        ASR1000-RP3         ok, active            00:25:14
R1                            unknown               00:25:14
F0        ASR1000-ESP100      ok, active            00:25:14
F1        ASR1000-ESP100      ok, standby           00:25:14

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         19041800            16.3(2r)
1         19041600            16.3(2r)
2         19041600            16.3(2r)
R0        17042115            16.9(5r)
R1        N/A                 N/A
F0        19051700            16.3(2r)
F1        19051700            16.3(2r)
============================================================
Dec 12 07:55:57.709: %PMAN-5

*** Unreset the Standby RP ***
*** POWER CYCLING RP3 !!! ***

Initializing Hardware ...

System integrity status: 9B710000  12030000  30FF0001


System Bootstrap, Version 16.9(5r), RELEASE SOFTWARE
Copyright (c) 1994-2019  by cisco Systems, Inc.

Current image running: Boot ROM0
Last reset cause: PowerOn

ASR1000-RP3 platform with 8388608 Kbytes of main memory

rommon 1 >

Total Time taken: 32min 25Sec

Trigger utility on Stdby Rp3, Keeping Active Rp3 on Rommon Prompt:
====================================================================
```

RP slot 1

```
==========
rommon 1 > boot harddisk:asr1000rpx86-universalk9.V1612_1_CSCVN77167.SPA.bin
File size is 0x4041ad8f
Located asr1000rpx86-universalk9.V1612_1_CSCVN77167.SPA.bin
Image size 1078046095 inode num 26, bks cnt 263195 blk size 8*512
################################################################################################################################################################

Boot image size = 1078046095 (0x4041ad8f) 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 16acc89c:916a2757:a9ac28c1:e5b88393:2ca73bab
        expected   16acc89c:916a2757:a9ac28c1:e5b88393:2ca73bab
Validating main package signatures

RSA Signed RELEASE Image Signature Verification Successful.
Image validated

This is the ACTIVE RP
Standby RP present - Hold it in reset

**************************************************
***         PSIRT FPGA UPGRADE REQUESTED         ***
***                                              ***
***        CURRENT CPLD VERSION: 17042115        ***
***                                              ***
***                UPGRADING FPGA                ***
***                                              ***
**************************************************
***                                              ***
***      WARNING !!  WARNING !! WARNING !!       ***
***                                              ***
*** DO NOT POWER CYCLE OR TURN OFF THE ROUTER !!! ***
***                                              ***
*** DO NOT ADD OR REMOVE CARDS FROM THE SYSTEM !! ***
***                                              ***
***  THIS MAY TAKE UP TO 20 MINUTES TO COMPLETE  ***
***                                              ***
**************************************************

****************************************
***  Upgrade completed on this card     ***
****************************************

              Restricted Rights Legend

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

           Cisco Systems, Inc.
           170 West Tasman Drive
           San Jose, California 95134-1706



Cisco IOS Software [Gibraltar], ASR1000 Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 16.12.1,
 CUST-SPECIAL:V1612_1_CSCVN77167

This software is supported for a limited time under special agreement with Cisco Systems, Inc.
CSCvn77167
Copyright (c) 1986-2019 by Cisco Systems, Inc.

Compiled Wed 11-Dec-19 02:06 by mcpre



This software version supports only Smart Licensing as the software licensing mechanism.


PLEASE READ THE FOLLOWING TERMS CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE,
```

```
AND/OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE
"SOFTWARE"), AND/OR USING SUCH SOFTWARE CONSTITUTES YOUR FULL
ACCEPTANCE OF THE FOLLOWING TERMS. YOU MUST NOT PROCEED FURTHER IF YOU
ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement
(EULA) and any relevant supplemental terms (SEULA) found at
http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.

You hereby acknowledge and agree that certain Software and/or features are
licensed for a particular term, that the license to such Software and/or
features is valid only for the applicable term and that such Software and/or
features may be shut down or otherwise terminated by Cisco after expiration
of the applicable license term (e.g., 90-day trial period). Cisco reserves
the right to terminate any such Software feature electronically or by any
other means available. While Cisco may provide alerts, it is your sole
responsibility to monitor your usage of any such term Software feature to
ensure that your systems and networks are prepared for a shutdown of the
Software feature.



All TCP AO KDF Tests Pass
============================================================
==                  ACTIVE RP                               ==
==  WAITING FOR ALL LINECARDS TO BOOT AFTER FPGA UPGRADE ==
==                                                          ==
==    DO NOT POWER CYCLE OR TURN OFF THE ROUTER !!!      ==
============================================================
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-6TGE         in slot 1 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-6TGE         in slot 1 - booting
Waiting for card ASR1000-6TGE         in slot 1 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - disconnecting
Waiting for card ASR1000-MIP100       in slot 0 - disconnecting
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - unknown
Waiting for card ASR1000-6TGE         in slot 1 - disconnecting
Waiting for card ASR1000-6TGE         in slot 1 - unknown
Waiting for card ASR1000-6TGE         in slot 1 - unknown
Waiting for card ASR1000-MIP100       in slot 0 - booting
Waiting for card ASR1000-MIP100       in slot 0 - booting
============================================================
Waiting for linecards to remain stable
............................................................
============================================================
============================================================
```

```
Chassis type: ASR1009-X

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1000-MIP100      ok                    00:26:31
1         ASR1000-6TGE        ok                    00:26:31
2         ASR1000-2T+20X1GE   ok                    00:26:31
R0                            unknown               00:26:31
R1        ASR1000-RP3         ok, active            00:26:31
F0        ASR1000-ESP100      ok, active            00:26:31
F1        ASR1000-ESP100      ok, standby           00:26:31

Slot      CPLD Version        Firmware Version
--------- ------------------- ----------------------------------------
0         19041800            16.3(2r)
1         19041600            16.3(2r)
2         19041600            16.3(2r)
R0        N/A                 N/A
R1        17042115            16.9(5r)
F0        19051700            16.3(2r)
F1        19051700            16.3(2r)
============================================================
Dec 12 08:32:13.779: %PMA

*** Unreset the Standby RP ***
*** POWER CYCLING RP3 !!! ***

Initializing Hardware ...

System integrity status: 9B710000  12030000  30FF0001


System Bootstrap, Version 16.9(5r), RELEASE SOFTWARE
Copyright (c) 1994-2019  by cisco Systems, Inc.

Current image running: Boot ROM0
Last reset cause: PowerOn

ASR1000-RP3 platform with 8388608 Kbytes of main memory

rommon 1 >
```

Step 7 (Optional) Ensure you have physical access to the router and manually power cyle the router. This step is only required if as part of the prerequisite you have determined that the **`Top Assy. Part Number`** value is less than **05**.

Step 8 After the CPLD upgrade, boot the router with the previously loaded IOS XE software image. For example : `asr1000rpx86-universalk9.16.12.01.SPA.bin`

```
rommon 1 > boot harddisk:asr1000rpx86-universalk9.16.12.01.SPA.bin
Warning: filesystem is not clean
File size is 0x3f4030db
Located asr1000rpx86-universalk9.16.12.01.SPA.bin
Image size 1061171419 inode num 20, bks cnt 259076 blk size 8*512
```

Step 9 Change the configuration register value to the value noted in **step 2**

```
Router#show version | in configuration
Configuration register is 0x0

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

```
Router(config)#end
```

Verifying CPLD Upgrade for ASR 1000 Modular Chassis

To verify the FPGA upgrade, use the following command:

```
Router#show platform
Chassis type: ASR1009-X

Slot      Type                State                 Insert time (ago)
--------- ------------------- --------------------- -----------------
0         ASR1000-MIP100      ok                    00:33:39
 0/0      EPA-QSFP-1X100GE    ok                    00:30:43
1         ASR1000-6TGE        ok                    00:33:39
 1/0      BUILT-IN-6TGE       ok                    00:31:40
2         ASR1000-2T+20X1GE   ok                    00:33:39
 2/0      BUILT-IN-2T+20X1GE  ok                    00:31:38
R0        ASR1000-RP3         ok, active            00:33:39
R1        ASR1000-RP3         ok, standby           00:33:39
F0        ASR1000-ESP100      ok, active            00:33:39
F1        ASR1000-ESP100      ok, standby           00:33:39
P0        ASR1000X-AC-1100W   ok                    00:32:28
P1        ASR1000X-AC-1100W   ok                    00:32:26
P2        Unknown             empty                 never
P3        Unknown             empty                 never
P4        Unknown             empty                 never
P5        Unknown             empty                 never
P6        ASR1000X-FAN        ok                    00:32:17
P7        ASR1000X-FAN        ok                    00:32:16
P8        ASR1000X-FAN        ok                    00:32:18

Slot      CPLD Version        Firmware Version
--------- ------------------- ------------------------------------
0         19041800            16.3(2r)
1         19041600            16.3(2r)
2         19041600            16.3(2r)
R0        19091111            16.9(5r)
R1        19091111            16.9(5r)
F0        19051700            16.3(2r)
F1        19051700            16.3(2r)
```

Note Verify the CPLD version with the platforms given in Check the CPLD Version for ASR 1000 Modular Chassis, on page 13.

Check the CPLD Version for ASR 1000 Modular Chassis

Table 1: Recommended CPLD Versions

PIDs	CPLD Versions
ASR1000-RP3	19091111

PIDs	CPLD Versions
ASR1000-ESP100	19051700
ASR1000-ESP200	19051700
ASR1000-ESP200-X	19041811
ASR1000-ESP100-X	19041811
ASR1000-MIP100	19041800
ASR1000-2T+20X1GE	19041600
ASR1000-6TGE	19041600

Note Do not perform power cycle or remove the power cable during the 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.

Information about Upgrading Cisco ASR 1000 Consolidated Chassis

This section provides instructions on how to address the Cisco Secure Boot Hardware Tampering Vulnerability on Cisco ASR 1000 consolidated chassis.

Note Complex Programmable Logic Device (CPLD) is also refered to as Field Programmable Gate Arrays (FPGA) and you find either CPLD or FPGA is used interchangeable in the folloing sections.

Prerequisites for Upgrading CPLD for ASR 1000 Consolidated Chassis

- Download the image from the CCO website and copy it to USB or bootflash of the router which is scheduled for the upgrade.
- Cisco ASR1001, ASR1002, and ASR1002-X Series routers are not affected by this PSIRT.

Note The platforms that are affected by this hardware vulnerability are listed in Table 1. It is strongly recommended to not run the IOS XE tool on any other platforms.

Upgrading CPLD for ASR 1000 Consolidated Chassis

Note Cisco recommends upgrading CPLD 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.

To upgrade CPLD, run the upgrade utility image:

Procedure

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.

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

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

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

```
Router#show version | in Configuration
Configuration register is 0x2102
WLC#

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

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

```
Router#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:ASR1K-fpga_prog.16.0.1.xe.bin
```

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

```
boot bootflash:ASR1K-fpga_prog.16.0.1.xe.bin
```

```
rommon 2 > boot bootflash:ASR1K-fpga_prog.16.0.1.xe.bin
File size is 0x015a3814
Located ASR1K-fpga_prog.16.0.1.xe.bin
Image size 22689812 inode num 32, bks cnt 5540 blk size 8*512
################################################################################################################################################################
Boot image size = 22689812 (0x15a3814) 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 c55a44e3:d0433d49:ef3e0f29:04956cc7:3232af02
expected c55a44e3:d0433d49:ef3e0f29:04956cc7:3232af02
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: ASR1001-X

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: 00000610
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

ASR1001-X platform with 4194304 Kbytes of main memory
```

Important **********

The following message confirms the upgrade is successful:

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

Retry the upgrade by issuing **Yes**.

```
Use can issue “y” or “Y” to retry.

Detected Board Type: ASR1001-HX
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: ASR1001-HX

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

ASR1001-HX platform with 8388608 Kbytes of main memory

rommon 1 >
```

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

Step 8 After 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-- asr1001x-universalk9.03.16.06.S.155-3.S6-ext.SPA.bin

rommon 2 > boot bootflash:asr1001x-universalk9.03.16.06.S.155-3.S6-ext.SPA.bin
```

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

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

Verifying CPLd Upgrade for ASR 1000 Consolidated Chassis

To verify the CPLD upgrade, use the following command:

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

Slot              CPLD version              FPGA version
------------------------------------------------------------
0                 19030215                  16051716
```

Note Verify the CPLD version with the platforms given in the CPLD Versions and Images table.

Table 2: CPLD Versions and Images

S. No	Platforms	CPLD Version	CCO URL for the CPLD Image
1	ASR1001-X	19060309	FPGA Upgrade Tool
2	ASR1002-HX	19030211	FPGA Upgrade Tool
3	ASR1001-HX	19030215	FPGA Upgrade Tool

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.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

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