Recover from a Boot Loop Caused by Image Corruption on Wave 2 and 11ax Access Points (CSCvx32806)

Contents

Introduction

Some Cisco access points (APs) may download a corrupt image via CAPWAP (Control and Provisioning of Wireless Access Points) from a 9800 series controller. Depending on the AP's software version, the AP may try to boot the corrupt image, resulting in a boot loop. This article explains how to recover access points that are stuck in a boot loop. To learn more on which products and deployments are susceptible to this problem and to learn how to upgrade safely without encountering the boot loop issue, please refer to the article Safely Upgrade Access Points, Avoiding Image Corruption That Causes Boot Loop.

This issue is documented as Field Notice: FN74109 - Access Point Image Corruption During CAPWAP Upgrade May Result in Boot Failu....

Problem Conditions

Not Affected Products

- Wireless LAN Controllers (WLCs): APs downloading from AireOS Wireless LAN Controllers are not affected
- Mobility Express, Embedded Wireless Controller
- APs - Aironet 1800/1540/1100AC series Wave 2 11ac APs and Wave1 11ac Access Points

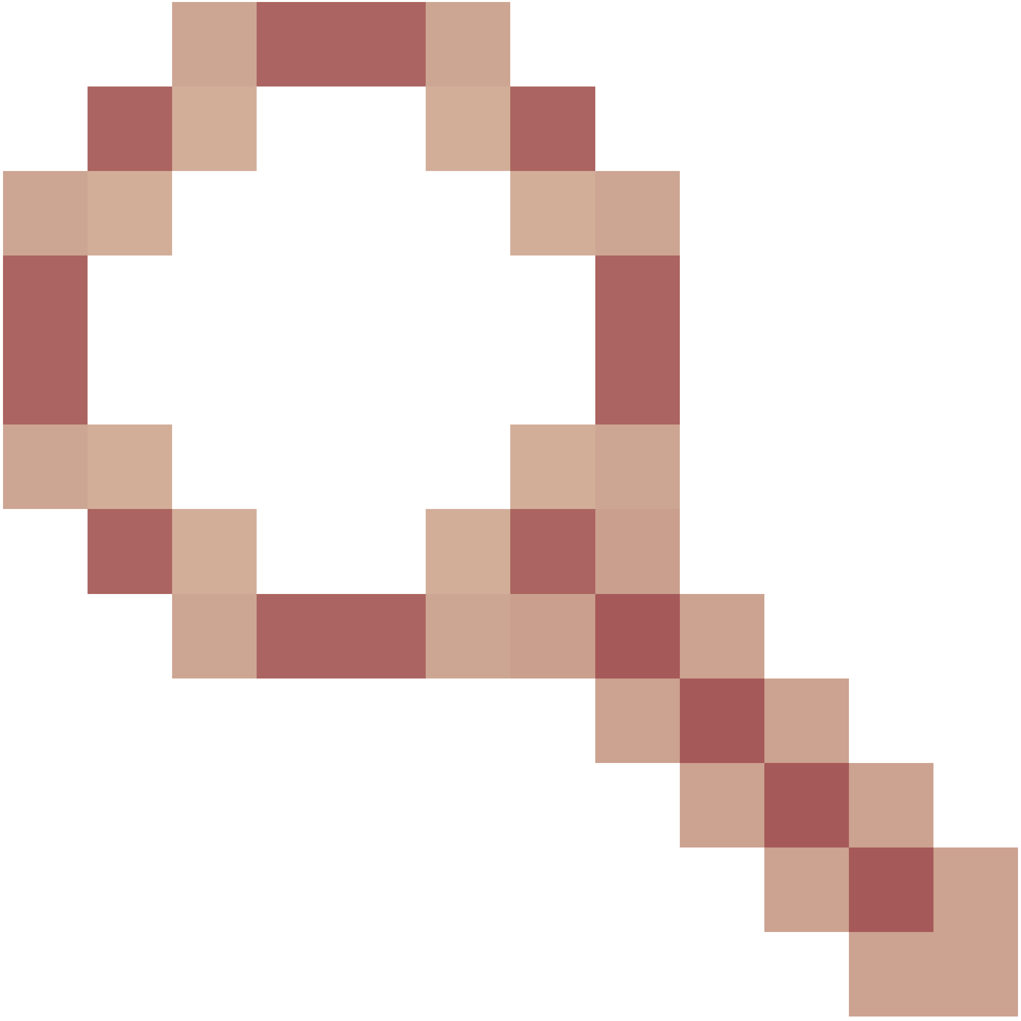
(1700/2700/3700/1570/IW3700) are not affected (even if these APs are registering to 9800 WLCs, they are not impacted)
- Wi-Fi 6E APs introduced since 2023: IW9167, IW9165, C9163

Affected Products

- WLC : APs download from Cisco Catalyst 9800 Series Wireless LAN Controllers may be affected
- APs : The following AP models registering to Cisco Catalyst 9800 Series Wireless LAN Controllers are affected :
  - Aironet Wave2 11ac Access Points (2800/3800/4800/1560/IW6330/ESW6300)
  - Catalyst 9100 Series Wi-Fi6 Access Points (9105/9115/9117/9120/9124/9130/WP-WIFI6/ISR-AP1101AX)
  - Catalyst 9100 Series Wi-FI6E Access Points (9136/9162/9164/9166)

Affected Versions: the Boot a Bad Image Syndrome

This problem, where the AP attempts to boot an image that it knows is corrupt, is addressed by the following



Cisco bug IDs: CSCvx32806
, CSCwc72021

, CSCwd90081

, which are fixed in the the following releases:

- 8.10.185.0 and above
- 17.3.7 and above
- 17.6.6 and above
- 17.9.3 and above
- 17.11.1 and above

Once the AP is upgraded to software with the above fixes, it may still download a corrupt image; however, it will not attempt to boot that image, but instead will continue to reattempt the download until it succeeds.

Symptoms

AP Console :

An AP that has already downloaded the corrupt image and is now in a boot loop, will show a console message similar to the following:

verify signature failed for /bootpart/part1/ramfs_data_cisco.cpio.lzma

or

verify signature failed for /bootpart/part2/ramfs_data_cisco.squashfs

Make a note of whether the message says "part1" or "part2" - this will indicate which boot partition is corrupt.

Syslog or Show logging :

If the access point was configured to log to an external syslog server, prior to the image download attempt, it will log the following error:

Image signature verification failure: -3

This error message can also be seen from the AP CLI (console or SSH), in the "show logging" output. If the logging buffer has been overwritten since the image update attempt, the error message may be seen in the syslog files stored in AP flash. If you see neither success nor failure messages in the show logging, then use one of the recovery methods on the AP to reinstall the desired image via TFTP or SFTP.

Cisco Switchport :

The APs in a boot loop state will show IEEE PD as shown below in the Show output of the AP's uplink switchport. (APs operating properly will show their model in the Device column, if using CDP or LLDP):

<#root>

```
switch#show power inline
Available:195.0(w)  Used:159.9(w)  Remaining:35.1(w)

Interface Admin  Oper       Power   Device              Class Max
                            (Watts)
--------- ------ ---------- ------- ------------------- ----- ----
Gi0/1     auto   on         15.4

Ieee PD

             4     30.0
Gi0/2     auto   on         24.1    C9115AXI-B          4     30.0
```

How To Recover APs That Are in a Boot Loop

Determine Whether the APs Have the Alt-boot Enhancement

If an AP has downloaded a corrupt image, and is attempting to boot it, it will exhibit one of two behaviors, depending on whether its u-boot (AP bootloader) has the Alt-boot (Alternate booot) enhancement

- Without Alt-boot: the AP will attempt indefinitely to boot the corrupt image, and will need to be recovered via its console port
- With Alt-boot: the AP will attempt to boot the corrupt image five times, then boot the image from its

backup partition. In this case, the AP can be recovered without console access, using one of the Alt-boot recovery methods documented below.

The Alt-boot u-boot enhancement is bundled in the following software releases:

- 9117/9130/9124: 8.10.190.0, 17.3.8+, 17.6.6+, 17.9.1+
- 9136: 17.9.1+
- 916x: all units have the Alt-boot enhancement
- 9105/9115/9120/2800/3800/4800/1560/6300: 8.10.190.0, 17.3.8+, 17.6.6+, 17.9.4

Note that, if an AP has downloaded an image that has the Alt-boot enhancement, its u-boot will be upgraded, even if the runtime image is corrupt. For example, consider this scenario:

- a 9130 AP has 17.3.4c installed (without the Alt-boot enhancement.)
- It then downloads a 17.9.5 image, but that image is corrupted during the download.
- Because 17.3.4c doesn't have the fix for the Boot a Bad Image Syndrome, the AP goes ahead and tries to boot the corrupt image.
- Booting the new image partition will cause the AP to upgrade to the 17.9.5 u-boot, before it tries to boot the bad runtime image.
- The AP will then attempt five times to boot the corrupt 17.9.5 runtime image.
- Then, because the AP now is running the 17.9.5 u-boot, the Alt-boot logic will switch the AP to boot the runtime image in its backup partition.
- The AP can now be recovered without console access.

Recovering APs That Are in a Boot Loop - With Alt-boot Enhancement

If your APs are in a boot loop, and if their U-boot has the Alt-boot Enhancement, then use one of the following procedures to recover them:

If SSH Is Enabled on the APs

1. Stage the desired AP image(s) on a TFTP or SFTP server that is accessible to the affected APs. See Table 4 in the Compatibility Matrix for the 15.3(3)J* AP version that maps to the desired Cisco IOS® XE version, then download the appropriate Lightweight AP Software image(s) for affected AP model(s) from software.cisco.com.
    1. For example, the 17.9.5 AP image for a CW9162 is ap1g6b-k9w8-tar.153-3.JPN4.tar.
2. Prevent the affected APs from joining a controller that is running the same software version as is in their corrupt partition. Thus, add a CAPWAP ACL on the AP switchport, to prevent the AP from again joining the controller. For example, an ACL similar to below can be applied on the AP's subnet's default gateway's interface:

```
Router#show running-config | section access-list 133
access-list 133 deny ip host <wlc_ip> any log
access-list 133 deny ip any host <wlc_ip> log
access-list 133 permit ip any any

Router#show running-config interface Vlan6
[ ... ]
interface Vlan6
ip address 192.168.6.1 255.255.255.0
ip access-group 133 in
```

3. Let the AP reboot with the corrupted image five times, after which it should switch to the working image in the backup partition.
   1. You can use the command **`show cdp neighbor <interface> detail`** on the AP's switch to see what version of code is in the AP's backup partition. (If the AP is booting the corrupt image, CDP won't come up on its port.)
4. Once the AP comes up with the working backup image it will try to join the controller, but won't be able to because of the ACL added in the step 2.
5. SSH into each affected AP (if a large number of APs are affected, this step can be automated via WLAN Poller.)
6. Now download the desired image onto the backup partition of the AP using the archive download command:
   ```
   archive download-sw /no-reload tftp://<ip-address>/<apimage>
   ```
   or
   ```
   archive download-sw /no-reload sftp://<ip-address>/<apimage>
   ```
   This will overwrite the corrupted image with the valid image. Once the image download completes, issue:
   test capwap restart
   This will restart the CAPWAP process, so that the AP will recognize the newly installed image.
7. Now remove the ACL, and have the AP join the controller. It will not download the image again.

If SSH Is Not Enabled on the APs, But the APs have the Alt-boot Enhancement

1. Make sure that the APs don't try to join a controller that is running the same software version as is in their corrupt partition. Thus, add a CAPWAP ACL on the AP switchport, to prevent the AP from again joining the controller.
2. Bring up a controller running a different software version than the AP's corrupt version.
   1. You can use the command **`show cdp neighbor <interface> detail`** on the AP's switch to see what version of code is in the AP's backup partition. (While the AP is booting the corrupt image, CDP won't come up on its port.)
   2. If it's not feasible to stage a controller running the AP's backup version, then (if 9800), at least stage a version with fixes for the Boot a Bad Image Syndrome and with Alt-boot.
   3. Another option would be to have an AireOS controller running 8.10.190.0 or above, as CAPWAP downloads from AireOS are not susceptible to image corruption.
3. Set things up so that the APs can discover the alternate controller - for example, via DHCP Option 43, an IP helper address, or DNS.
   1. Do note that, if the alternate controller is running a Cisco IOS XE version that differs from the AP's backup, the AP will be susceptible to downloading a corrupt image, so iterate this process for any such APs that may be newly corrupted.
4. Once the APs join the alternate controller, then download the desired image onto the APs:
   1. Stage the desired AP image(s) on a TFTP or SFTP server that is accessible to the affected APs. See Table 4 in the Compatibility Matrix for the 15.3(3)J* AP version that maps to the desired Cisco IOS XE version, then download the appropriate Lightweight AP Software image(s) for affected AP model(s) from software.cisco.com.
      1. For example, the 17.9.5 AP image for a CW9162 is ap1g6b-k9w8-tar.153-3.JPN4.tar.
   2. Enable ssh on the affected APs, and ssh into each affected AP (if a large number of APs are affected, this step can be automated via WLAN Poller.)
      1. Now download the desired image onto the backup partition of the AP using the archive download command:
         ```
         archive download-sw /no-reload tftp://<ip-address>/<apimage>
         ```
         or
         ```
         archive download-sw /no-reload sftp://<ip-address>/<apimage>
         ```
         This will overwrite the corrupted image with the valid image.
      2. Once the image download completes, issue:

        `test capwap restart`
        This will restart the CAPWAP process, so that the AP will recognize the newly installed image.
    3. As an alternative to executing **archive download-sw** on the APs, you may use the following controller commands to get the APs to download the desired image from a TFTP server:
        1. In Cisco IOS XE: **`ap name`** ***`APNAME`*** **`tftp-downgrade`** ***`ip.addr.of.server imagename.tar`***
        2. In AireOS: **`config ap tftp-downgrade`** ***`ip.addr.of.server imagename.tar APNAME`***
        3. Monitor the TFTP server logs to verify that each AP has successfully downloaded the image. Once the download completes, each AP will reload, running the newly downloaded image.

5. Remove the ACL that was installed in step 1, and have the APs join the desired controller.

Recovery via Console

If the AP is in a boot loop, and if the AP does not have the Alt-boot enhancement, then the AP must be recovered via console.

For All AP Models: Determine Which Boot Partition Is Corrupt

First, ascertain which boot partition is corrupt.

1. Connect to the AP console.
2. Watch the AP attempt to boot, until you see the message
   `verify signature failed for /bootpart/part1/ramfs_data_cisco.cpio.lzma`
   or
   `verify signature failed for /bootpart/part2/ramfs_data_cisco.cpio.lzma`
   (the message may say "*ramfs_data_cisco.squashfs*" instead of "*ramfs_data_cisco.cpio.lzma*"
3. Make a note of which partition, **part1** or or **part2**, is corrupt

For AP Models 9117, 9124, 9130, 9136

1. While connected to the console, power cycle the AP.

2. During bootup, when you see ***Hit ESC key to stop autoboot,*** press the Escape key

3. You should see one of these prompts:

   (BTLDR) #
   or
   (u-boot)>

4. Run these commands

```
(u-boot)> or (BTLDR)# setenv mtdids nand0=nand0 && setenv mtdparts mtdparts=nand0:0x40000000@0x0(f
(u-boot)> or (BTLDR)# ubi remove part1   (or part2 if corrupted image is in part2)
(u-boot)> or (BTLDR)# ubi create part1   (or part2 if corrupted image is in part2)
(u-boot)> or (BTLDR)# reset
```

For AP Models 2802, 3802, 4800, 9105, 9115, 9120

1. While connected to the console, power cycle the AP.
2. During bootup, when you see ***Hit ESC key to stop autoboot,*** press the Escape key
3. This should bring you to (u-boot)> prompt.
4. Run these commands

```
(u-boot)> ubi part fs
(u-boot)> ubi remove part1  (or part2 if corrupted image is in part2)
(u-boot)> ubi create part1  (or part2 if corrupted image is in part2)
(u-boot)> boot
```

Frequently Asked Questions

Q1) My APs are all connected to their 9800 via a high-speed, low-latency, low-loss LAN connection. Do I still need to execute the above?

This issue has only been reported when upgrading APs over a WAN connection.

Q2) I have new out-of-box APs. How can I deploy them without encountering this issue?

New out-of-box APs downloading code over a lossy WAN link will also be susceptible to the issue, if they were manufactured prior to December, 2023. It is recommended to stage these APs first with a local WLC.

Q3) I have more questions about this issue. To whom may I direct them?

A: Send email to fn74109-questions@cisco.com.