IOS AP Image Download Fails Due to Expired Image Signing Certificate Post December 4th, 2022 (CSCwd80290)

Contents

Introduction

This document provides details on IOS access point (AP) join failures, seen with both AireOS and C9800 Wireless LAN Controllers (WLCs), after December 4, 2022. This issue is tracked by Cisco bug CSCwd80290 and the Field Notice FN72524 and is caused by an AP image signing certificate validation failure.

Affected Products

This problem affects all lightweight access points that run IOS - these include: 802.11ac Wave 1 APs (IW3702/3700/2700/1700/1570 series) and earlier APs including 700/1530/1550/3600/2600/1600/3500/AP802/AP803 series. The affected lightweight IOS images were built from December 2012 through November 2022. AireOS, Catalyst 9800 series and Converged Access controllers are affected. APs that run AP-COS (802.11ac Wave 2, Wi-Fi 6, Wi-Fi 6E APs) are not affected, nor are IOS APs in autonomous mode.

Problem

When IOS APs are upgraded or downgraded via CAPWAP, after December 4, 2022, they may get stuck in an image download loop, and thereby fail to join the WLC, due to a failure to validate the signing certificate in the downloaded image.

Root Cause

The image signing certificates bundled in the AP IOS images were issued on December 4, 2012, and expired on December 4, 2022. IOS APs use this certificate to validate the image downloaded from the WLC, before installing the software on the AP. So, after December 4, 2022, when an AP downloads code due to software upgrade/downgrade or due to moving between WLCs running different versions, the AP will fail to validate the image and will remain in a download image loop indefinitely. The problem is seen for all AireOS and IOS-XE versions.

Symptoms

To verify whether you are running into this problem, first check on the WLC for APs stuck in Downloading status. Then, to positively identify the problem, ssh, telnet or console into the affected APs and view their logs (or look for AP logs on your syslog server.)

On an AireOS WLC

On the WLC, **`show ap image status`** (AireOS 8.10) will show the affected APs in "Downloading" status.

In 8.5, use **`show ap image all`** which will show a nonzero number of APs in "Downloading".

```
(AireOS WLC-8.5) >show ap image all Total number of APs.............................. 1 Number
of APs Initiated....................................... 0
Downloading.................................... 1
Predownloading................................. 0 Completed
predownloading........................ 0 Not Supported.................................. 0
Failed to Predownload.......................... 0 Predownload Predownload Flexconnect AP Name
Primary Image Backup Image Status Version Next Retry Time Retry Count Predownload --------------
---- -------------- -------------- --------------- -------------- ---------------- ------------
-------------- AP1700 8.5.182.0 0.0.0.0 None None NA NA (AireOS WLC-8.10) >show ap image status
Total number of APs............................ X Total AP's
Downloading.......................... 1 AP Name Primary Image Download Status -----------------
- -------------- ---------------- CAP3702E.4CD4 17.3.6.76 Downloading
```

On an IOS-XE C9800 WLC

C9800#show ap summary

```
9800-L#show ap summary AP Name Slots AP Model Ethernet MAC Radio MAC Location Country IP Address
State -----------------------------------------------------------------------------------------
-----------------------------------------------------------------------------------------------
- AP2702E 2 2702E 0081.c4fb.2e74 843d.c673.10d0 default location 192.168.202.105 Downloading
```

The AP logs will show errors similar to the following when encountering this problem:

On a SHA-1 AP (manufactured prior to mid-2014):

```
*Dec 6 21:35:24.259: Using SHA-1 signed certificate for image signing validation.
*Dec 6 21:35:24.327: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has
failed. The certificate (SN: XX) has expired. Validity period ended on 21:37:36 UTC Dec 4 2022
*Dec 6 21:35:24.327: Image signing certificate validation failed (1A).
```

```
*Dec 6 21:35:24.327: Failed to validate signature
*Dec 6 21:35:24.327: Digital Signature Failed Validation (flash:/update/ap3g2-k9w8-mx.153-
3.JPJ9/final_hash)
*Dec 6 21:35:24.327: AP image integrity check FAILED
```

On a SHA-2 AP (manufactured after mid-2014):

```
*Dec 6 08:47:20.159: Using SHA-2 signed certificate for image signing validation.
*Dec 6 08:47:20.223: DTLS_CLIENT_ERROR: ../capwap/base_capwap/dtls/base_capwap_dtls_record.c:169
Pkt too old last_seq_num : 11116,Received sequence num: 1 distance: -11115
*Dec 6 08:47:20.227: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has
failed. The certificate (SN: XX) has expired. Validity period ended on 21:43:46 UTC Dec 4 2022
*Dec 6 08:47:20.227: Image signing certificate validation failed (1A).
*Dec 6 08:47:20.231: Failed to validate signature
*Dec 6 08:47:20.231: Digital Signature Failed Validation (flash:/update/ap3g2-k9w8-mx.153-
3.JPJ7c/final_hash)
*Dec 6 08:47:20.231: AP image integrity check FAILED
```

Workaround

If you are not running fixed software, follow these steps to allow the IOS APs to join.

1. Disable NTP, to prevent the controller from automatically setting its time forward.

```
AireOS: (AireOS WLC)>show time make a note of all configured NTP servers, and delete each one:
(AireOS WLC)>config time ntp delete <INDEX_Number> IOS-XE: C9800#show run | i ntp ntp server ip
<NTP_SERVER_IP1> C9800#config terminal (config)#no ntp server ip <NTP_SERVER_IP1> ! for each
configured NTP server
```

2. Change the date on the WLC to something before December 4, 2022 but not before November 1, 2022, as it may invalidate the certificate in the controller or in newer APs.

```
(AireOS WLC)> config time manual 12/02/22 00:00:00 C9800#clock set 00:00:00 2 Dec 2022
```

3. Verify that the time on the WLC has changed

```
(AireOS WLC)> show time Time............................................. Fri Dec 2 00:00:02
2022 C9800#show clock 00:00:02.573 <TIMEZONE> Fri Dec 2 2022
```

4. Wait for all of the APs to come up in Registered state with the new image.

> **Note: In some cases, an AP reboot may be required after date change to get the AP joined. But please be sure to wait at least 30 minutes to allow AP to join back before rebooting APs**

5. Enable NTP again

```
(AireOS WLC)>config time ntp server 1 <NTP_SERVER_IP1> C9800#configure terminal (config)#ntp
server ip <NTP_SERVER_IP1>
```

6. Save the configuration

```
(AireOS WLC)>save config Are you sure you want to save? (y/n) y C9800#write memory
```

7. Re-verify clock on the WLC

```
(AireOS WLC)>show time C9800# show clock
```

Upgrading to Fixed Software

On an AireOS WLC

1. If you have any APs stuck in downloading, then set the controller time back so APs can complete downloading and come up in Registered State before upgrading to the software. See the workaround section above for details on setting the time backIf, for operational reasons, you are unable to set the time back, then block the affected IOS APs from attempting to join the controller, for example by shutting down their switchports, or installing an ACL to block CAPWAP.
2. Now that no APs are in the Downloading state, make sure that the WLC's time is set to the current time (re-enable NTP.)
3. Install the fixed software on the AireOS WLC (8.10.183.0 or above; or, if unable to upgrade from 8.5, use 8.5.182.7, if using 8.5 mainline, or 8.5.182.105, for 8.5 IRCM.). Refer to the links below to download the fixed software. 8.10 8540: https://software.cisco.com/download/home/286284728/type/280926587/release/8.10.183.0 5520: https://software.cisco.com/download/home/286284738/type/280926587/release/8.10.183.0 3504: https://software.cisco.com/download/home/286312601/type/280926587/release/8.10.183.0 vWLC: https://software.cisco.com/download/home/284464214/type/280926587/release/8.10.183.08.5 (hidden posts) 8.5.182.7 (8.5 mainline): https://software.cisco.com/download/specialrelease/8f166c6d88b9f77aabb63f78affa9749. 8.5.182.105 (8.5 IRCM): https://software.cisco.com/download/specialrelease/bc334964055fbd9440834f008e5aca34.
4. (Optionally) Before rebooting, predownload the fixed software to the joined APs.
5. Reboot the WLC.
6. If you shut down AP switchports or blocked CAPWAP, remove the blocks to allow the IOS APs to rejoin and upgrade.

On an IOS-XE 9800 WLC

1. Download the 17.3.6, 17.6.4, 17.9.2 IOS-XE software to 9800 flash. Refer to the Recommended IOS-XE Releases for C9800 WLCs to choose the version best suited for your environment based on AP Models in your environment and features in use.

2. Download the 17.3.6 APSP7 or 17.6.4 APSP1 or 17.9.2 APSP1 file (with IOS AP fix) to 9800 flash.

- 17.3.6: 17.3.6 APSP7 via CSCwd83653/CSCwe10047 (fix also included in APSP2 and APSP5)

9800-40: https://software.cisco.com/download/home/286316412/type/286325254/release/17.3.6

9800-80: https://software.cisco.com/download/home/286321396/type/286325254/release/17.3.6

9800-CL: https://software.cisco.com/download/home/286322605/type/286325254/release/17.3.6

9800-L: https://software.cisco.com/download/home/286323430/type/286325254/release/17.3.6

- 17.6.4: 17.6.4 APSP1 (for IW3702) via CSCwd87305

9800-40: https://software.cisco.com/download/home/286316412/type/286325254/release/17.6.4

9800-80: https://software.cisco.com/download/home/286321396/type/286325254/release/17.6.4

9800-CL: https://software.cisco.com/download/home/286322605/type/286325254/release/17.6.4

9800-L: https://software.cisco.com/download/home/286323430/type/286325254/release/17.6.4

- 17.9.2:17.9.2 APSP1 (for IW3702) via CSCwd87612

9800-40: https://software.cisco.com/download/home/286322605/type/286325254/release/17.9.2

9800-80: https://software.cisco.com/download/home/286321396/type/286325254/release/17.9.2

9800-CL: https://software.cisco.com/download/home/286322605/type/286325254/release/17.9.2

9800-L: https://software.cisco.com/download/home/286323430/type/286325254/release/17.9.2

Note:
1) 17.3.6 APSP7 includes fixes for multiple bugs (CSCvx32806, CSCwc32182, CSCvz99036, CSCwd37092, CSCwc78435, CSCwc88148) in addition to CSCwd80290
2) 17.6.4 APSP1 includes fixes for multiple bugs (CSCwc73090, CSCwc71198, CSCwc78435, CSCwd40731, CSCvx32806) in addition to CSCwd80290 (for IW3700).

3. Unless 17.3.6 is already installed, install 17.3.6 IOS-XE now and reload.

```
C9800#install add file bootflash:/C9800-L-universalk9_wlc.17.03.06.SPA.bin activate commit
```

4. After the 9800 reboots - if the controller time had been set back in time, now set its time to current (re-enable NTP.)

5 Install APSP7 to recover the IOS APs:

```
C9800#install add file bootflash:/C9800-universalk9_wlc.17.03.06.CSCwe10047 .SPA.apsp.bin
C9800#install activate file bootflash:/C9800-universalk9_wlc.17.03.06.CSCwe10047 .SPA.apsp.bin
C9800#install commit
```

Frequently Asked Questions (FAQ)

- **Are my current registered APs going to disconnect or fail to join due to this issue?**
  APs running the same version as the WLC will continue to operate without problems and will boot and join normally. This issue only impacts the image validation process done as part of an image upgrade.

- **Is AP predownload impacted?**

Yes. Since the AP predownload involves downloading of an image to AP and validation of the image by AP, the same expired certificate and image validation failure is encountered.

- **What service impact does the change of time have? Can a customer do this at noon, or should they schedule a maintenance window with some downtime and impact on services?**
  Changing the controller time has no operational impact on AP joins and wireless client connectivity. However, DNA Center Assurance, CMX and Cisco (DNA) Spaces may be impacted. Once APs are joined and the time is set back to the current time, these services are expected to recover.

- **What if I cannot set the time back on my production controller?**
  Set up a staging WLC (vWLC or 9800-CL also works) with the same code version as the production WLC. Revert time on the staging WLC and join APs to the staging WLC. Once the APs downloads code and moves to Registered state on the staging WLC, move the APs to the production WLC.

- **Do I need to change the time to install the fixed version?**

Only with AireOS, if the APs are stuck in downloading state.. Refer to the section on *Upgrading to fixed software* for further details.

- **What happens if I add a new AP ?**
  If the new AP has installed on it the same version as the controller, the AP should join without problems.
  On the other hand, if the version does not match, the AP will try to download the corresponding image. If the code on the controller does not have the fixed AP bundled images, this will cause the AP to fail the upgrade as described, and the workaround will be necessary.
  If the controller has been upgraded to one of the fixed versions, new APs can be added normally, and complete the upgrade process.

- **What will happen for units received from RMA?**
  This is equivalent to adding new a AP: if you are running controller version with the AP image fix, they will join and upgrade normally.
  Otherwise, apply the time workaround.

- **Do I need to keep the time modified for operation?**
  No, once the APs have completed the upgrade process, you can set the controller back to the current time, and re-enable NTP.

- **I am seeing this error on the AP log %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Certificate chain validation has failed. The certificate (SN: xx) is not yet valid Validity period starts on HH:MM:SS UTC Mar 1 2022". Is this same symptom or new symptom?**

This error indicates that the clock on the WLC is set behind March 1, 2022 which is the start date of the certificate (in this case). This date will vary depending on when the WLC was manufactured or when the Self-Signed Certificate on the Virtual WLC was generated.

Modify the clock on the WLC to make the certificate valid.

- **What is Cisco doing to prevent this problem from recurring?**
  We are completing a full audit across all Enterprise products, to identify any similar problem that could have been undetected, and implement corrective actions
  Additionally, changes have been applied to IOS AP image bundle process, to correct this problem.