IOS AP-Image-Download aufgrund abgelaufener Image-Signaturzertifikatpost am 4. Dezember 2022 fehlgeschlagen (CSCwd80290)

Inhalt

Einleitung

Dieses Dokument enthält Details zu Verbindungsfehlern von IOS Access Points (APs), die bei AireOS- und C9800 Wireless LAN Controllern (WLCs) nach dem 4. Dezember 2022 aufgetreten sind. Dieses Problem wird durch den Cisco Bug CSCwd80290 und die Problemhinweis-Nr. FN72524 verfolgt und wird durch einen Fehler bei der Validierung des Zertifikats für die AP-Image-Signatur verursacht.

Betroffene Produkte

Dieses Problem betrifft alle Lightweight Access Points, auf denen IOS ausgeführt wird, darunter: 802.11ac Wave 1 APs (Serie IW3702/3700/2700/1700/1570) und frühere APs, einschließlich 700/1530/1 Serie 550/3600/2600/1600/3500/AP802/AP803. Die betroffenen Lightweight IOS Images wurden von Dezember 2012 bis November 2022 erstellt. Betroffen sind AireOS-, Catalyst 9800- und Converged Access Controller. APs, die AP-COS ausführen (802.11ac Wave 2, Wi-Fi 6, Wi-Fi 6E-APs) sind davon nicht betroffen, ebenso wenig wie IOS-APs im autonomen Modus.

Problem

Wenn IOS-APs nach dem 4. Dezember 2022 über CAPWAP aktualisiert oder herabgestuft werden, bleiben sie möglicherweise in einer Image-Download-Schleife stecken und treten dem WLC nicht bei, da das Signaturzertifikat im heruntergeladenen Image nicht validiert wurde.

Ursache

Die in den AP-IOS-Images gebündelten Signaturzertifikate wurden am 4. Dezember 2012 ausgestellt und sind am 4. Dezember 2022 abgelaufen. IOS-APs verwenden dieses Zertifikat, um das vom WLC heruntergeladene Image zu validieren, bevor sie die Software auf dem AP installieren. Wenn also nach dem 4. Dezember 2022 ein Access Point aufgrund eines Software-Upgrades/Downgrades oder aufgrund einer Verschiebung zwischen WLCs mit unterschiedlichen Versionen Code herunterlädt, kann der Access Point das Image nicht validieren und bleibt auf unbestimmte Zeit in einer Download-Image-Schleife. Das Problem tritt bei allen AireOS- und IOS-XE-Versionen auf.

Symptome

Um zu überprüfen, ob dieses Problem auftritt, überprüfen Sie zunächst den WLC auf APs, die im Status "Herunterladen" feststecken. Anschließend können Sie das Problem mithilfe von ssh, telnet oder console in den betroffenen APs identifizieren und deren Protokolle anzeigen (oder auf Ihrem Syslog-Server nach AP-Protokollen suchen).

Auf einem AireOS-WLC

Auf dem WLC zeigt **show ap image status** (AireOS 8.10) die betroffenen APs im Status "Downloading" (Herunterladen) an.

In 8.5, verwenden **show ap image all**, die eine ungleich null Anzahl von APs zeigen 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
```

Auf einem IOS-XE C9800 WLC

C9800#show ap Zusammenfassung

```
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
```

Die AP-Protokolle zeigen Fehler wie die folgenden an, wenn auf dieses Problem trifft:

Auf einem SHA-1 AP (hergestellt vor Mitte 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
```

Auf einem SHA-2 AP (hergestellt nach Mitte 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
```

Problemumgehung

Wenn Sie keine feste Software ausführen, befolgen Sie diese Schritte, um den IOS APs die Teilnahme zu ermöglichen.

1. Deaktivieren Sie NTP, um zu verhindern, dass der Controller die Zeitvorgabe automatisch festlegt.

```
AireOS: (AireOS WLC)>show time make a note of all configured NTP servers, and delete each one:
(AireOS WLC)>config time ntp delete
```

2. Ändern Sie das Datum auf dem WLC auf einen Wert vor dem 4. Dezember 2022, jedoch nicht vor dem 1. November 2022, da es das Zertifikat im Controller oder in neueren APs ungültig machen kann.

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

3. Vergewissern Sie sich, dass sich die Zeit am WLC geändert hat.

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

4. Warten Sie, bis alle Access Points im registrierten Zustand mit dem neuen Image angezeigt werden.

> **Hinweis: In einigen Fällen kann nach der Datumsänderung ein Neustart des Access Points erforderlich sein, um den Access Point in den Access Point einzubinden. Warten Sie jedoch mindestens 30 Minuten, bis der Access Point wieder angemeldet ist, bevor Sie die Access Points neu starten.**

5. Aktivieren Sie NTP erneut.

```
(AireOS WLC)>config time ntp server 1
```

6. Speichern der Konfiguration

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

7. Überprüfen Sie die Uhr am WLC erneut.

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

Upgrade auf festkonfigurierte Software

Auf einem AireOS-WLC

1. Wenn beim Herunterladen APs blockiert sind, stellen Sie die Controller-Zeit zurück, damit APs den Download abschließen und im registrierten Zustand hochgefahren werden können, bevor Sie ein Upgrade auf die Software durchführen. Weitere Informationen zum Zurücksetzen der Zeit finden Sie im Abschnitt zur Problemumgehung weiter oben.Wenn Sie aus betrieblichen Gründen die Zeit nicht zurücksetzen können, blockieren Sie den Versuch der betroffenen IOS-APs, dem Controller beizutreten, z. B. indem Sie deren Switch-Ports herunterfahren oder eine ACL installieren, um CAPWAP zu blockieren.
2. Da sich keine APs im Download-Zustand befinden, stellen Sie sicher, dass die WLC-Zeit auf die aktuelle Zeit eingestellt ist (NTP erneut aktivieren).
3. Installieren Sie die feste Software auf dem AireOS WLC (8.10.183.0 oder höher; oder, falls kein Upgrade von 8.5 möglich ist, verwenden Sie 8.5.182.7, falls Sie 8.5 Mainline oder 8.5.182.105 verwenden, für 8.5 IRCM.). Klicken Sie auf die nachstehenden Links, um die Software mit der korrekten Konfiguration herunterzuladen. 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 (versteckte Beiträge) 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. (Optional) Laden Sie vor dem Neustart die fixe Software auf die verbundenen APs vorab herunter.
5. Starten Sie den WLC neu.
6. Wenn Sie die AP-Switch-Ports herunterfahren oder CAPWAP blockieren, entfernen Sie die Blöcke, damit die IOS-APs wieder beitreten und ein Upgrade durchführen können..

Auf einem IOS-XE 9800 WLC

1. Laden Sie die IOS-XE-Software 17.3.6, 17.6.4 und 17.9.2 auf den 9800 Flash herunter. Unter Empfohlene IOS-XE-Versionen für C9800 WLCs finden Sie die Version, die für Ihre Umgebung

am besten geeignet ist, basierend auf den AP-Modellen in Ihrer Umgebung und den verwendeten Funktionen.

2. Laden Sie die Datei 17.3.6 APSP7 oder 17.6.4 APSP1 oder 17.9.2 APSP1 (mit IOS AP Fix) auf 9800 Flash herunter.

- 17.3.6: 17.3.6 APSP7 über CSCwd83653/CSCwe10047 (Fix auch in APSP2 und APSP5 enthalten)

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 (für IW3702) über 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 (für IW3702) über 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

Anmerkung:
1) 17.3.6 APSP7 enthält Fixes für mehrere Bugs (CSCvx32806, CSCwc32182, CSCvz99036, CSCwd37092, CSCww c78435, CSCwc88148) zusätzlich zu CSCwd80290
2) 17.6.4 APSP1 enthält Fixes für mehrere Fehler (CSCwc73090, CSCwc71198, CSCwc78435, CSCwd40731, CSC vx32806) und CSCwd80290 (für IW3700).

3. Sofern 17.3.6 nicht bereits installiert ist, installieren Sie jetzt 17.3.6 IOS-XE und laden Sie es erneut.

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

4. Nach dem Neustart des 9800: Wenn die Zeit des Controllers zurückgesetzt wurde, stellen Sie sie jetzt auf die aktuelle Zeit ein (NTP erneut aktivieren).

5 Installieren Sie APSP7, um die IOS-APs wiederherzustellen:

```
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
```

Häufig gestellte Fragen

- **Werden meine derzeit registrierten APs aufgrund dieses Problems getrennt oder können sie nicht beitreten?**
  APs, die dieselbe Version wie der WLC ausführen, funktionieren problemlos weiter und werden normal gebootet und verbunden. Dieses Problem wirkt sich nur auf den Image-Validierungsprozess aus, der im Rahmen eines Image-Upgrades durchgeführt wird.

- **Ist der AP-Vorabdownload beeinträchtigt?**

Ja. Da beim AP-Vorabdownload ein Image auf den Access Point heruntergeladen und das Image vom Access Point validiert wird, treten dasselbe abgelaufene Zertifikat und der gleiche Fehler bei der Image-Validierung auf.

- **Welche Auswirkungen hat der Zeitwechsel auf den Service? Kann ein Kunde diese Aufgabe am Mittag erledigen, oder sollte er ein Wartungsfenster mit Ausfallzeiten und Auswirkungen auf die Services planen?**
  Eine Änderung der Controller-Zeit hat keine Auswirkungen auf die AP-Verbindungen und die Wireless-Client-Verbindungen. Dies kann jedoch Auswirkungen auf DNA Center Assurance, CMX und Cisco (DNA) Spaces haben. Sobald die Access Points hinzugefügt und die Zeit auf die aktuelle Zeit zurückgesetzt werden, wird erwartet, dass sich diese Services erholen.

- **Was passiert, wenn ich die Zeit nicht auf meinem Produktionscontroller zurücksetzen kann?**
  Richten Sie einen Staging-WLC (vWLC oder 9800-CL funktioniert auch) mit der gleichen Codeversion wie der Produktions-WLC ein. Zeit auf dem Staging-WLC zurücksetzen und APs mit dem Staging-WLC verbinden Sobald die APs Code herunterladen und auf dem Staging-WLC in den registrierten Status wechseln, verschieben Sie die APs in den Produktions-WLC.

- **Muss ich die Zeit ändern, um die fixe Version zu installieren?**

Nur mit AireOS, wenn die APs im Download-Status feststecken. Weitere Informationen finden Sie im Abschnitt *Upgrade auf feste Software*.

- **Was passiert, wenn ich einen neuen Access Point hinzufüge?**
  Wenn der neue Access Point auf dem Gerät mit der gleichen Version wie der Controller installiert wurde, sollte der Access Point problemlos hinzugefügt werden.
  Wenn die Version jedoch nicht übereinstimmt, versucht der Access Point, das entsprechende Image herunterzuladen. Wenn der Code auf dem Controller nicht über die gebündelten Images mit dem festen Access Point verfügt, schlägt das Upgrade wie beschrieben fehl, und die Problemumgehung ist erforderlich.
  Wenn für den Controller ein Upgrade auf eine der festen Versionen durchgeführt wurde, können neue APs normal hinzugefügt werden, und der Upgrade-Prozess wird abgeschlossen.

- **Was geschieht mit den Einheiten, die von der RMA erhalten werden?**
  Dies entspricht dem Hinzufügen eines neuen Access Points: Wenn Sie die Controller-Version mit dem AP-Image-Fix ausführen, erfolgt der Beitritt zum Access Point und das Upgrade normal.

Ansonsten wenden Sie die Zeit Workaround.

- **Muss die Zeit für den Betrieb geändert werden?**
  Nein. Sobald die APs den Upgrade-Prozess abgeschlossen haben, können Sie den Controller auf die aktuelle Zeit zurücksetzen und NTP erneut aktivieren.

- **Ich sehe diesen Fehler im AP-Protokoll %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID: Fehler bei der Validierung der Zertifikatskette. Das Zertifikat (SN: xx) ist noch nicht gültig Gültigkeitszeitraum beginnt am HH:MM:SS UTC Mar 1 2022". Handelt es sich um dasselbe oder ein neues Symptom?**

Dieser Fehler zeigt an, dass die Uhr auf dem WLC hinter dem 1. März 2022 eingestellt ist, dem Startdatum des Zertifikats (in diesem Fall). Dieses Datum hängt davon ab, wann der WLC hergestellt wurde oder wann das selbstsignierte Zertifikat auf dem virtuellen WLC generiert wurde.

Ändern Sie die Uhr auf dem WLC, um das Zertifikat gültig zu machen.

- **Was unternimmt Cisco, um eine Wiederholung dieses Problems zu verhindern?**
  Wir führen derzeit eine umfassende Prüfung aller Enterprise-Produkte durch, um ähnliche Probleme zu identifizieren, die unentdeckt geblieben sein könnten, und um Korrekturmaßnahmen zu ergreifen.
  Darüber hinaus wurden Änderungen am IOS AP-Image-Paketprozess vorgenommen, um dieses Problem zu beheben.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.