IOS AP-image downloaden mislukt vanwege verlopen image Signing Certificate Post 4 december 2022 (CSCwd80290)

Inhoud

Inleiding

Dit document bevat informatie over IOS access point (AP)-feeds bij storingen die worden gezien met zowel AireOS- als C9800 draadloze LAN-controllers (WLC's) na 4 december 2022. Deze kwestie wordt gevolgd door Cisco-bug CSCwd80290 en de melding uit het veld FN72524 en wordt veroorzaakt door een fout in de validering van het AP-beeldondertekeningscertificaat.

Betrokken producten

Dit probleem heeft betrekking op alle lichtgewicht access points waarop IOS wordt uitgevoerd, zoals: 802.11ac Wave 1 AP's (IW3702/3700/2700/1700/1570 Series) en eerdere AP's, waaronder 700/1530/1550/3600/2600/1600/3500/AP800 3 series. De betrokken lichtgewicht IOS-beelden werden gebouwd van december 2012 tot november 2022. AireOS, Catalyst 9800 Series en geconvergeerde toegangscontrollers worden beïnvloed. AP's waarop AP-COS (802.11ac Wave 2, Wi-Fi 6, Wi-Fi 6E AP's) wordt uitgevoerd, worden niet beïnvloed, noch zijn IOS AP's in autonome modus.

Probleem

Wanneer IOS AP's worden geüpgraded of gedowngraded via CAPWAP, na 4 december 2022, kunnen ze vastzitten in een image download loop, en daardoor falen om zich aan te sluiten bij de WLC, vanwege een falen om het ondertekeningscertificaat in het gedownloade beeld te valideren.

Hoofdoorzaak

De gebundelde afbeeldingsondertekeningscertificaten in de AP IOS-afbeeldingen zijn uitgegeven op 4 december 2012 en zijn verlopen op 4 december 2022. IOS AP's gebruiken dit certificaat om de van de WLC gedownload afbeelding te valideren, voordat ze de software op de AP installeren. Dus na 4 december 2022, wanneer een AP code downloadt vanwege software upgrade/downgrade of vanwege het verplaatsen tussen WLC's met verschillende versies, zal de AP de afbeelding niet valideren en zal ze oneindig in een downloadbeeldlus blijven. Het probleem wordt gezien voor alle versies AireOS en IOS-XE.

Symptomen

Om te verifiëren of u dit probleem tegenkomt, controleer eerst WLC voor APs die in het Downloaden status worden geplakt. Vervolgens, om het probleem, ssh, telnet of console op een positieve manier te identificeren in de betreffende AP's en hun logs te bekijken (of te zoeken naar AP logs op uw syslogserver.)

Op een AireOS WLC

Op de WLC, **toon ap image status** (AireOS 8.10) zal tonen de aangetaste APs in "Downloaden" status.

In 8.5, gebruik **tonen ap beeld** die een nonzero aantal APs in "het Downloaden"zal tonen.

```
(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
```

Op een IOS-XE C980 WLC

C9800#show app samenvatting

```
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
```

De AP logboeken zullen fouten tonen gelijkend op het volgende wanneer het ontmoeten van dit probleem:

Op een SHA-1 AP (geproduceerd vóór medio 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
```

Op een SHA-2 AP (vervaardigd na medio 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
```

Tijdelijke oplossing

Als u geen vaste software gebruikt, volg dan deze stappen om de IOS AP's toe te staan toe te treden.

1. Schakel NTP uit om te voorkomen dat de controller automatisch de tijd vooruit instelt.

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

2. Verander de datum op de WLC naar iets voor 4 december 2022, maar niet voor 1 november 2022, omdat het certificaat in de controller of in nieuwere AP's ongeldig kan maken.

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

3. Controleer dat de tijd op de WLC is gewijzigd

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

4. Wacht totdat alle toegangspunten zijn geregistreerd met de nieuwe afbeelding.

> **Opmerking: in bepaalde gevallen moet het toegangspunt na de datumwijziging opnieuw worden opgestart om zich bij het toegangspunt aan te sluiten. Maar houd er rekening mee dat u minimaal 30 minuten moet wachten voordat AP zich kan aanmelden voor herstart van AP's**

5. NTP opnieuw inschakelen

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

6. De configuratie opslaan

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

7. Controleer de klok op de WLC opnieuw

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

Upgraden naar vaste software

Op een AireOS WLC

1. Als er nog AP's vastzitten in het downloaden, stel dan de controller tijd terug zodat AP's het downloaden kunnen voltooien en komen in Registered State voordat ze upgraden naar de software. Zie de tijdelijke oplossing hierboven voor meer informatie over het terugstellen van de tijdAls, om operationele redenen, u niet in staat bent om de tijd terug te zetten, dan blokkeert de betreffende IOS APs van het proberen om zich aan te sluiten bij de controller, bijvoorbeeld door hun switchports te sluiten, of het installeren van een ACL om CAPWAP te blokkeren.
2. Nu geen APs in de Downloadstaat zijn, zorg ervoor dat de tijd van WLC aan de huidige tijd wordt geplaatst (re-laat NTP toe.)
3. Installeer de vaste software op de AireOS WLC (8.10.183.0 of hoger; of gebruik, als u niet kunt upgraden van 8.5, 8.5.182.7, als u 8.5 mainline gebruikt, of 8.5.182.105, voor 8.5 IRCM.). Raadpleeg de onderstaande koppelingen om de vaste software te downloaden. 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 (verborgen berichten) 8.5.182.7 (hoofdlijn 8.5): https://software.cisco.com/download/specialrelease/8f166c6d88b9f77aabb63f78affa9749. 8.5.182.105 (8.5 IRCM): https://software.cisco.com/download/specialrelease/bc334964055fbd9440834f008e5aca34.
4. (Optioneel) Voor het opnieuw opstarten, download de vaste software vooraf naar de aangesloten AP's.
5. Reboot de WLC.
6. Als u AP-switchpoorten uitschakelt of CAPWAP blokkeert, verwijder dan de blokken om de IOS AP's weer bij elkaar te kunnen voegen en te upgraden.

Op een IOS-XE 9800 WLC

1. Download de software 17.3.6, 17.6.4, 17.9.2 IOS-XE naar 9800 flitser. Raadpleeg de Aanbevolen IOS-XE releases voor C9800 WLC's om de versie te kiezen die het meest geschikt is voor uw omgeving, gebaseerd op AP-modellen in uw omgeving en functies in gebruik.

2. Download het 17.3.6 APSP7- of 17.6.4 APSP1- of 17.9.2 APSP1-bestand (met IOS AP fix) naar 9800 flitser.

- 17.3.6: 17.3.6 APSP7 via CSCwd83653/CSCwe10047 (fix ook opgenomen in APSP2 en 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 (voor 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 (voor 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

Opmerking:
1) 17.3.6 APSP7 omvat fixes voor meerdere bugs (CSCvx32806, CSCwc32182, CSCvz99036, CSCwd37092, CSCwc78435, CSCwc8148) naast CSCwd80290
2) 17.6.4 APSP1 omvat fixes voor meerdere bugs (CSCwc73090, CSCwc71198, CSCwc78435, CSCwd40731, CSCvx32806) naast CSCwd80290 (voor IW370) .

3. Tenzij 17.3.6 al is geïnstalleerd, installeert u IOS-XE 17.3.6 nu en opnieuw.

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

4. Na de 9800 herstart - als de controller-tijd was teruggezet in de tijd, stel nu de tijd in op huidige (NTP opnieuw inschakelen).

5 Installeer APSP7 om de IOS APs te herstellen:

```
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
```

Veelgestelde vragen (FAQ)

- **Gaan mijn huidige geregistreerde AP's de verbinding verbreken of niet toetreden vanwege dit probleem?**
  AP's met dezelfde versie als de WLC zullen zonder problemen blijven werken en zullen opstarten en zich normaal aansluiten. Dit probleem heeft alleen invloed op het proces voor de validatie van afbeeldingen dat als onderdeel van een upgrade van het image wordt uitgevoerd.

- **Is AP predownload beïnvloed?**

Ja. Aangezien de AP predownload het downloaden van een beeld aan AP en de bevestiging van het beeld door AP impliceert, wordt de zelfde verlopen certificaat en de mislukking van de beeldbevestiging ontmoet.

- **Welke invloed heeft de verandering van de tijd op de dienstverlening? Kan een klant dit om 12.00 uur doen, of moeten ze een onderhoudsvenster plannen met wat uitvaltijd en impact op de diensten?**
  Het wijzigen van de controller tijd heeft geen operationele impact op AP joins en draadloze client connectiviteit. De ruimtes van DNA Center Assurance, CMX en Cisco (DNA) kunnen echter worden beïnvloed. Zodra AP's zijn aangesloten en de tijd is teruggezet naar de huidige tijd, wordt verwacht dat deze services herstellen.

- **Wat als ik de tijd niet kan terugzetten op mijn productiecontroller?**
  Stel een staging WLC (vWLC of 9800-CL werkt ook) in met dezelfde codeversie als de productie WLC. Keer tijd op de opvoerende WLC om en sluit zich aan bij AP's aan de opvoerende WLC. Zodra de APs downloadt code en beweegt naar Geregistreerde staat op het opvoeren WLC, verplaats de APs naar de productie WLC.

- **Moet ik de tijd wijzigen om de vaste versie te installeren?**

Alleen met AireOS, als de AP's vastzitten in de downloadstatus. Raadpleeg het gedeelte over het *upgraden naar vaste software* voor meer informatie.

- **Wat gebeurt er als ik een nieuwe AP toevoegt?**
  Als het nieuwe toegangspunt dezelfde versie heeft geïnstalleerd als de controller, moet het toegangspunt probleemloos worden aangesloten.
  Als de versie niet overeenkomt, probeert het toegangspunt de betreffende afbeelding te downloaden. Als de code op de controller niet de vaste AP gebundelde beelden heeft, zal dit ervoor zorgen dat het AP de upgrade mislukt zoals beschreven, en zal de tijdelijke oplossing nodig zijn.
  Als de controller is geüpgraded naar een van de vaste versies, kunnen er normaal nieuwe AP's worden toegevoegd en kan het upgradeproces worden voltooid.

- **Wat gebeurt er met de eenheden die van RMA worden ontvangen?**
  Dit staat gelijk aan het toevoegen van nieuwe AP: als u controller versie met de AP image fix draait, zullen ze zich normaal aansluiten en upgraden.
  Anders past u de tijdelijke oplossing toe.

- **Moet ik de tijd voor de werking aangepast houden?**
  Nee, zodra de AP's het upgradeproces hebben voltooid, kunt u de controller terugzetten naar de huidige tijd en NTP opnieuw inschakelen.

- **Ik zie deze fout op het AP log %PKI-3-CERTIFICAAT_INGELDIG_NOT_YET_GELDIG: De validatie van de certificaatketen is mislukt. Het certificaat (SN: xx) is nog niet geldig Geldigheidsperiode begint op UU:MM:SS UTC Mar 1 2022". Is dit hetzelfde symptoom of een nieuw symptoom?**

Deze fout geeft aan dat de klok op de WLC is ingesteld achter 1 maart 2022, wat de begindatum is van het certificaat (in dit geval). Deze datum zal variëren afhankelijk van wanneer de WLC werd geproduceerd of toen het zelfondertekende certificaat op de Virtual WLC werd gegenereerd.

Wijzig de klok op de WLC om het certificaat geldig te maken.

- **Wat doet Cisco om te voorkomen dat dit probleem opnieuw optreedt?**
  We zijn bezig met een volledige audit van alle Enterprise-producten, om elk soortgelijk probleem te identificeren dat onontdekt had kunnen zijn, en om corrigerende maatregelen te implementeren
  Daarnaast zijn wijzigingen aangebracht in het IOS AP-image bundelproces om dit probleem te verhelpen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.