Échec du téléchargement de l'image IOS AP en raison de l'expiration du certificat de signature d'image après le 4 décembre 2022 (CSCwd80290)

Table des matières

Introduction

Ce document fournit des détails sur les échecs de jonction de point d'accès IOS, vus avec AireOS et les contrôleurs LAN sans fil (WLC) C9800, après le 4 décembre 2022. Ce problème est suivi par le bogue Cisco CSCwd80290 et l'avis de champ FN72524 et est causé par un échec de validation de certificat de signature d'image AP.

Produits concernés

Ce problème affecte tous les points d'accès légers qui exécutent IOS, notamment les points d'accès 802.11ac de phase 1 (série IW3702/3700/2700/1700/1570) et les points d'accès antérieurs, notamment les points d'accès 700/1530/1550/3600/2600/1600/3500/AP802/AP8 Série 03. Les images IOS légères concernées ont été créées de décembre 2012 à novembre 2022. AireOS, la gamme Catalyst 9800 et les contrôleurs d'accès convergé sont affectés. Les points d'accès qui exécutent AP-COS (points d'accès 802.11ac phase 2, Wi-Fi 6, Wi-Fi 6E) ne sont pas affectés, pas plus que les points d'accès IOS en mode autonome.

Problème

Lorsque les points d'accès IOS sont mis à niveau ou rétrogradés via CAPWAP, après le 4 décembre 2022, ils peuvent se retrouver coincés dans une boucle de téléchargement d'image, et ainsi ne pas rejoindre le WLC, en raison d'un échec de validation du certificat de signature dans l'image téléchargée.

Cause première

Les certificats de signature d'image regroupés dans les images IOS AP ont été émis le 4 décembre 2012 et ont expiré le 4 décembre 2022. Les AP IOS utilisent ce certificat pour valider l'image téléchargée à partir du WLC, avant d'installer le logiciel sur l'AP. Ainsi, après le 4 décembre 2022, lorsqu'un AP télécharge du code en raison d'une mise à niveau/rétrogradation logicielle ou en raison d'un déplacement entre des WLC exécutant différentes versions, l'AP ne pourra pas valider l'image et restera dans une boucle d'image de téléchargement indéfiniment. Le problème est visible pour toutes les versions d'AireOS et d'IOS-XE.

Symptômes

Pour vérifier si vous rencontrez ce problème, vérifiez d'abord sur le WLC pour les AP bloqués dans l'état de téléchargement. Ensuite, pour identifier le problème de manière positive, ssh, telnet ou console dans les AP affectés et afficher leurs journaux (ou rechercher les journaux AP sur votre serveur syslog.)

Sur un WLC AireOS

Sur le WLC, show ap image status (AireOS 8.10) affichera les AP affectés dans l'état « Downloading ».

Dans 8.5, utilisez show ap image all qui affichera un nombre non nul d'AP dans "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
AP Name            Primary Image  Backup Image   Status          Version        Next Retry Time  Retry
------------------ -------------- -------------- --------------- -------------- ---------------- ------
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
```

Sur un WLC C9800 IOS-XE

C9800#show ap summary

```
9800-L#show ap summary

AP Name                             Slots    AP Model  Ethernet MAC    Radio MAC       Location
-----------------------------------------------------------------------------------------------------
AP2702E                               2      2702E     0081.c4fb.2e74  843d.c673.10d0  default location
```

Les journaux d'AP afficheront des erreurs similaires à celles-ci en rencontrant ce problème :

Sur un point d'accès SHA-1 (fabriqué avant la mi-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 c
*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_
*Dec 6 21:35:24.327: AP image integrity check FAILED
```

Sur un point d'accès SHA-2 (fabriqué après la mi-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 to
*Dec 6 08:47:20.227: %PKI-3-CERTIFICATE_INVALID_EXPIRED: Certificate chain validation has failed. The c
*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
*Dec 6 08:47:20.231: AP image integrity check FAILED
```

Solution de contournement

Si vous n'exécutez pas de logiciel fixe, suivez ces étapes pour permettre aux AP IOS de se joindre.

1. Désactivez NTP pour empêcher le contrôleur de régler automatiquement son avance temporelle.

```
AireOS:
(AireOS WLC)>show time

make a note of all configured NTP servers, and delete each one:

(AireOS WLC)>config time ntp delete
```

```
      IOS-XE: C9800#show run | i ntp ntp server ip
```

```
       C9800#config terminal (config)#no ntp server ip
```

```
        ! for each configured NTP server
```

2. Modifiez la date sur le WLC à quelque chose avant le 4 décembre 2022 mais pas avant le 1er novembre 2022, car il peut invalider le certificat dans le contrôleur ou dans les AP plus récents.

```
(AireOS WLC)> config time manual 12/02/22 00:00:00

C9800#clock set 00:00:00 2 Dec 2022
```

3. Vérifiez que l'heure sur le WLC a changé

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

```
C9800#show clock
00:00:02.573
```

```
Fri Dec 2 2022
```

4. Attendez que tous les points d’accès apparaissent à l’état Registered avec la nouvelle image.

Remarque : dans certains cas, un redémarrage de l'AP peut être nécessaire après le changement de date pour joindre l'AP. Mais assurez-vous d'attendre au moins 30 minutes pour permettre à AP de se joindre à nouveau avant de redémarrer les AP

---

5. Réactivez le protocole NTP

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

```
C9800#configure terminal (config)#ntp server ip
```

6. Enregistrez la configuration

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

```
C9800#write memory
```

7. Vérifiez à nouveau l'horloge sur le WLC

```
(AireOS WLC)>show time
```

```
C9800# show clock
```

Mise à niveau vers un logiciel fixe

Sur un WLC AireOS

1. Si vous avez des AP bloqués dans le téléchargement, alors réglez le temps du contrôleur afin que les AP puissent terminer le téléchargement et revenir à l'état Registered avant la mise à niveau vers le logiciel.
    1. Reportez-vous à la section de contournement ci-dessus pour plus d'informations sur la configuration du retour arrière

    2. Si, pour des raisons opérationnelles, vous ne parvenez pas à remonter le temps, empêchez les AP IOS affectés d'essayer de joindre le contrôleur, par exemple en arrêtant leurs ports de commutateur, ou en installant une ACL pour bloquer CAPWAP.

2. Maintenant qu'aucun AP n'est à l'état Downloading, assurez-vous que l'heure du WLC est définie sur l'heure actuelle (réactivez NTP.)
3. Installez le logiciel fixe sur le WLC AireOS (8.10.183.0 ou supérieur ; ou, si vous ne pouvez pas effectuer la mise à niveau à partir de 8.5, utilisez 8.5.182.7, si vous utilisez 8.5 mainline, ou 8.5.182.105, pour 8.5 IRCM.). Reportez-vous aux liens ci-dessous pour télécharger le logiciel fixe.
    - 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/8.10.183.0

    - 8.5 (publications cachées)

    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. (Facultatif) Avant de redémarrer, prétéléchargez le logiciel fixe sur les points d'accès joints.
5. Redémarrez le WLC.
6. Si vous arrêtez les ports de commutation AP ou bloquez CAPWAP, supprimez les blocs

pour permettre aux AP IOS de se joindre à nouveau et de mettre à niveau.

Sur un WLC IOS-XE 9800

1. Téléchargez les versions 17.3.6, 17.6.4 et 17.9.2 du logiciel IOS-XE vers la mémoire flash 9800. Référez-vous aux Versions IOS-XE recommandées pour les WLC C9800 pour choisir la version la mieux adaptée à votre environnement en fonction des modèles AP dans votre environnement et des fonctionnalités en cours d'utilisation.

2. Téléchargez le fichier 17.3.6 APSP7 ou 17.6.4 APSP1 ou 17.9.2 APSP1 (avec correctif IOS AP) vers la mémoire flash 9800.

- 17.3.6 : 17.3.6 APSP7 via CSCwd83653/CSCwe10047 (correctif également inclus dans APSP2 et 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 (pour 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 (pour 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

Remarque :
1) 17.3.6 APSP7 inclut des correctifs pour plusieurs bogues (CSCvx32806, CSCwc32182, CSCvz99036, CSCwd37092, CSCwc78435, CSCwc8148) en plus de CSCwd80290
2) 17.6.4 APSP1 inclut des correctifs pour plusieurs bogues (CSCwc73090, CSCwc71198, CSCwc78435, CSCwd40731, CSCvx32806) en plus de CSCwd80290 (pour IW3700).

---

3. Sauf si 17.3.6 est déjà installé, installez 17.3.6 IOS-XE maintenant et rechargez.

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

4. Après le redémarrage du 9800 - si l'heure du contrôleur avait été repoussée dans le temps, définissez maintenant son heure sur l'heure actuelle (réactivez NTP).

5 Installez APSP7 pour récupérer les points d'accès IOS :

```
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
```

Foire aux questions (FAQ)

- Mes points d'accès actuellement enregistrés vont-ils se déconnecter ou ne pas se joindre en raison de ce problème ?
  Les AP exécutant la même version que le WLC continueront à fonctionner sans problème et démarreront et se joindront normalement. Ce problème affecte uniquement le processus de validation d'image effectué dans le cadre d'une mise à niveau d'image.

- Le prétéléchargement AP est-il affecté ?

Oui. Puisque le prétéléchargement AP implique le téléchargement d'une image sur AP et la validation de l'image par AP, le même certificat expiré et l'échec de validation d'image est rencontré.

- Quel est l'impact du changement d'heure sur le service ? Un client peut-il effectuer cette opération à midi ou doit-il planifier une période de maintenance avec des interruptions et un impact sur les services ?
  La modification de l'heure du contrôleur n'a aucun impact opérationnel sur les jonctions AP et la connectivité du client sans fil. Toutefois, les solutions DNA Center Assurance, CMX et Cisco (DNA) Spaces peuvent être affectées. Une fois que les points d'accès sont joints et que l'heure est reportée à l'heure actuelle, ces services sont censés se rétablir.

- Que faire si je ne parviens pas à redéfinir l'heure sur mon contrôleur de production ?
  Configurez un WLC intermédiaire (vWLC ou 9800-CL fonctionne également) avec la même version de code que le WLC de production. Rétablir le temps sur le WLC intermédiaire et joindre les AP au WLC intermédiaire. Une fois que les AP téléchargent le code et passent à l'état Registered sur le WLC intermédiaire, déplacez les AP vers le WLC de production.

- Dois-je modifier l'heure d'installation de la version corrigée ?

Uniquement avec AireOS, si les AP sont bloqués en état de téléchargement. Référez-vous à la section sur la Mise à niveau vers un logiciel fixe pour plus de détails.

- Que se passe-t-il si j'ajoute un nouveau point d'accès ?
  Si le nouveau point d'accès a installé sur lui la même version que le contrôleur, le point d'accès devrait se joindre sans problèmes.
  D'autre part, si la version ne correspond pas, l'AP essaiera de télécharger l'image correspondante. Si le code sur le contrôleur n'a pas les images fixes AP groupées, cela fera échouer l'AP à la mise à niveau comme décrit, et la solution de contournement sera nécessaire.
  Si le contrôleur a été mis à niveau vers l'une des versions fixes, de nouveaux AP peuvent être ajoutés normalement, et terminer le processus de mise à niveau.

- Que se passe-t-il pour les unités reçues de RMA ?
  Cela équivaut à ajouter un nouveau point d'accès : si vous exécutez la version du contrôleur avec le correctif d'image du point d'accès, ils se joindront et se mettront à niveau normalement.
  Sinon, appliquez la solution de contournement temporel.

- Dois-je conserver l'heure modifiée pour le fonctionnement ?
  Non, une fois que les AP ont terminé le processus de mise à niveau, vous pouvez réinitialiser le contrôleur à l'heure actuelle, et réactiver NTP.

- Je vois cette erreur dans le journal AP %PKI-3-CERTIFICATE_INVALID_NOT_YET_VALID : La validation de la chaîne de certificats a échoué. Le certificat (SN: xx) n'est pas encore valide. La période de validité commence le HH:MM:SS UTC Mar 1 2022. Est-ce le même symptôme ou un nouveau symptôme ?

Cette erreur indique que l'horloge sur le WLC est placée derrière le 1er mars 2022 qui est la date de début du certificat (dans ce cas). Cette date varie selon le moment où le WLC a été fabriqué ou quand le certificat auto-signé sur le WLC virtuel a été généré.

Modifiez l'horloge sur le WLC pour rendre le certificat valide.

- Que fait Cisco pour empêcher que ce problème ne se reproduise ?
  Nous procédons actuellement à un audit complet de tous les produits de l'entreprise afin d'identifier tout problème similaire qui aurait pu ne pas être détecté et de mettre en oeuvre des actions correctives
  En outre, des modifications ont été appliquées au processus d'ensemble d'images IOS AP, pour corriger ce problème.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.